CA IdentityMinder™

Manuel d'administration

r12.6.1

Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA IdentityMinder ™
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting (CA UAR)
- CA CloudMinder™ Identity Management
- GovernanceMinder (anciennement CA Role & Compliance Manager)

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 3: Tâches d'administration 41

Chapitre 4: Utilisateurs 85

Chapitre 8: Comptes de terminaux gérés 177

Chapitre 9: Rôles de provisionnement 217

Chapitre 15: Policy Xpress 329

Chapitre 16: Génération de rapports 347

Chapitre 17: CA User Activity Reporting 395

Chapitre 18: Flux de travaux 411

Chapitre 22: Tâches système 573

Chapitre 1: Planification de rôles

Aux fins de planification de vos rôles, définissez le type de rôles nécessaires à votre activité ou à votre organisation, ainsi que la méthode de délégation de la gestion des utilisateurs et de leur accès aux applications. En fonction de ces choix, définissez les caractéristiques de chaque rôle.

Ce chapitre traite des sujets suivants :

Décisions concernant les rôles

La section suivante inclut des informations pour vous aider à prendre des décisions informées sur les rôles.

Objectif des rôles

Pour utiliser des rôles de manière efficace, tenez compte des types de questions suivantes sur les besoins des utilisateurs et les responsabilités des administrateurs :

- Quels sont les départements et les organisations qui doivent gérer des utilisateurs ?
- Quels sont les comptes supplémentaires dont les utilisateurs auront besoin dans les terminaux gérés ?
- Quels sont les utilisateurs qui doivent être administrateurs d'autres utilisateurs ?
- Qui doit gérer les administrateurs ?
- Quelles sont les tâches d'administration et d'accès nécessaires à chaque rôle ?
- Qui doit créer les rôles et les tâches ?
- Comment puis-je utiliser des rôles pour déléguer des tâches ?

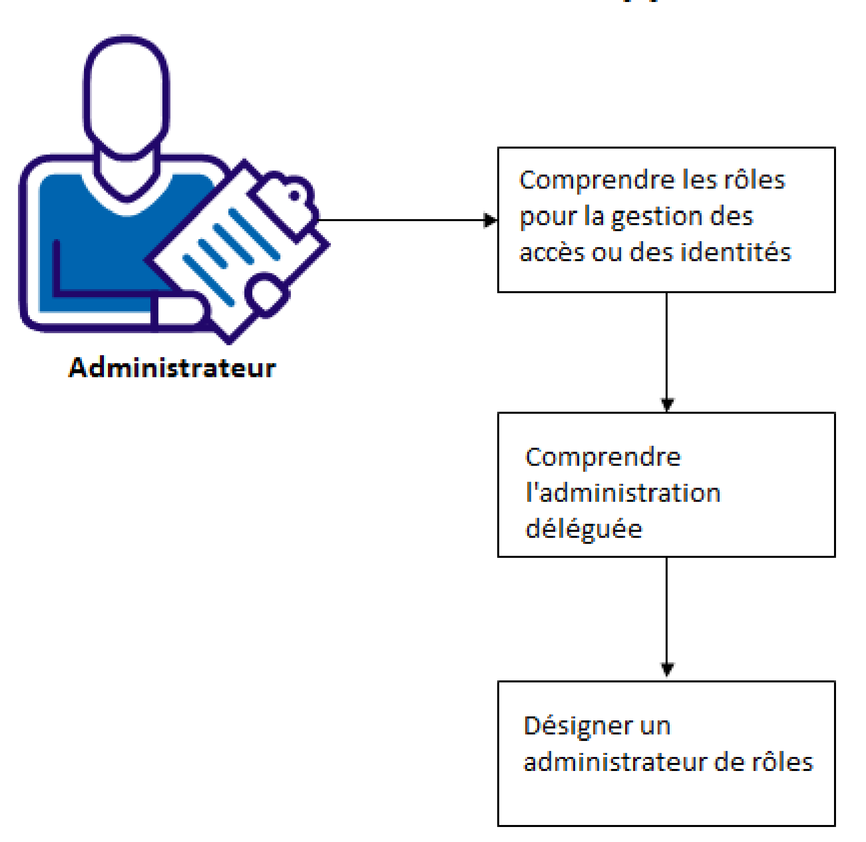
  La dernière question concerne le partage de la gestion des utilisateurs et l'octroi d'accès aux applications. Vous trouverez plus d'informations sur le modèle de délégation sous la rubrique Délégation d'administration.

En fonction des réponses à ces questions, vous pouvez définir le nombre et le type de rôles nécessaires.

Création d'administrateurs supplémentaires

Vous pouvez être le seul responsable de l'octroi de tous les rôles à des utilisateurs dans votre système. Vous pouvez également partager cette tâche en désignant d'autres administrateurs. Cette approche est appelée *délégation d'administration*.

Le schéma suivant contient des informations importantes et les étapes à suivre pour la création et la configuration d'administrateurs supplémentaires.



Les rubriques suivantes décrivent la création d'administrateurs supplémentaires :

- Rôles pour la gestion des identités ou des accès (page 19)
- Délégation d'administration (page 19)
- Désignation d'un administrateur de rôles (page 20)

Rôles pour la gestion des identités ou des accès

Pour activer la gestion des identités d'utilisateurs et de leur accès à d'autres comptes, CA Cloud Access Manager fournit deux types de rôles. Un rôle d'administration permet à un utilisateur de gérer des utilisateurs ; il peut par exemple modifier le mot de passe d'un utilisateur ou son appartenance à un groupe. Rôles d'administration peuvent également inclure les tâches qui s'affichent dans la console d'utilisateur. Un rôle de provisionnement permet à un utilisateur d'accéder à d'autres applications métier, comme un système de messagerie.

D'autres détails sur les rôles figurent dans le tableau suivant :

Type de rôle	Objectif
Rôle d'administration	Contient des tâches d'administration qu'un utilisateur détenant ce rôle peut effectuer dans CA Cloud Access Manager, telles que les tâches de gestion d'utilisateurs.
Rôle de provisionnement	Contient des modèles de compte qui définissent des comptes existant dans des terminaux gérés, tels qu'un système de messagerie. Ces modèles de compte définissent également la méthode de mappage des attributs d'utilisateurs vers les comptes.
Rôle d'accès	Les rôles d'accès permettent de fournir des droits dans CA IdentityMinder ou une autre application. Par exemple, vous pouvez utiliser les rôles d'accès pour effectuer les actions suivantes : ■ Fournir l'accès indirect à un attribut d'utilisateur ■ Créer des expressions complexes ■ Définir un attribut de profil qu'une autre application peut utiliser pour déterminer des droits

Délégation d'administration

La délégation d'administration est l'utilisation de rôles visant à partager le travail de gestion des utilisateurs et d'attribution d'accès à des applications.

Pour chaque rôle dans le système, un utilisateur peut utiliser l'une ou plusieurs des fonctions suivantes :properties

Fonction	Définition
Propriétaire d'un rôle	Modifie le rôle.
Administrateur de rôles	Affecte le rôle à des utilisateurs et à d'autres administrateurs de rôle.

Fonction	Définition
Membre avec rôle	Utilise le rôle pour effectuer les tâches d'administration ou d'accès ou pour utiliser un compte de terminal.

En divisant ces fonctions parmi plusieurs utilisateurs, vous pouvez partager le travail de gestion d'un rôle. Par exemple, vous pouvez décider que les administrateurs de niveau inférieur gèrent l'appartenance aux rôles et que les administrateurs de niveau supérieur modifient les rôles.

Vous pouvez implémenter la délégation d'administration de l'une des manières suivantes :

- Désignez directement un utilisateur comme administrateur d'un rôle spécifique.
- Configurez des *règles d'administration* pour un rôle. Les règles d'administration définissent les utilisateurs pouvant être administrateurs d'un rôle. Le système crée automatiquement des administrateurs supplémentaires lorsque les utilisateurs sont conformes aux critères spécifiés dans les règles.

  Remarque : Seul un administrateur disposant de droits de modification d'un rôle peut configurer des règles d'administration pour ce rôle. Généralement, les administrateurs système effectuent cette tâche. Pour configurer des règles d'administration qui délèguent automatiquement l'administration d'un rôle, consultez la section intitulée Rôles d'administration dans la rubrique Informations de référence de l'Aide en ligne.

Désignation d'un administrateur de rôles

Vous pouvez désigner un utilisateur comme administrateur d'un rôle. Cet administrateur peut alors affecter le rôle à d'autres utilisateurs.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur en tant qu'utilisateur avec des tâches de gestion de rôles.
2. Sélectionnez Rôles et tâches.
3. Sélectionnez l'une des tâches suivantes :
   - Rôles d'administration, Modifier les membres/administrateurs avec rôle d'administration
   - Rôles de provisionnement, Modifier les membres/administrateurs avec rôle de provisionnement
   - Rôles d'accès, Modifier les membres/administrateurs avec rôle d'accès

Une fenêtre de recherche apparaît.

4. Sélectionnez le rôle que vous souhaitez affecter à l'utilisateur.
5. Cliquez sur l'onglet Administrateurs.

   Une liste d'administrateurs de rôles actuels s'affiche.

6. Cliquez sur Ajouter un utilisateur

   Une fenêtre de recherche apparaît.

7. Recherchez l'utilisateur que vous voulez ajouter en tant qu'administrateur et cliquez sur Sélectionner.

   Une liste mise à jour d'administrateurs de rôles s'affiche.

8. Cliquez sur Soumettre.

   L'utilisateur devient un administrateur du rôle. Cette étape termine le processus de délégation d'administration d'un rôle de provisionnement. L'administrateur peut maintenant affecter le rôle à d'autres utilisateurs, en octroyant l'accès aux comptes de terminal associés.

Etapes de délégation

Après avoir défini l'utilisation des rôles en fonction de leur objectif, la délégation d'administration intervient comme suit :

1. Un administrateur crée le rôle avec des règles pour l'utilisateur propriétaire d'un rôle, un administrateur, ou un membre.
2. Si des modifications sont nécessaires, un propriétaire peut modifier le rôle.
3. L'administrateur de rôles :
   - Affecte d'autres administrateurs de rôles (facultatif).
   - Affecte d'autres membres avec rôles (facultatif).

   Certains utilisateurs sont déjà administrateurs de rôles ou membres avec rôle, car ils observent les règles définies dans le rôle.

4. Utilisation du rôle par un membre avec rôle :
   - Un membre avec rôle d'administration gère des utilisateurs et d'autres objets dans l'environnement CA Identity Manager.
   - Un membre avec rôle d'accès exécute des fonctions dans des applications métier.
   - Un membre avec rôle de provisionnement utilise les comptes définis par des stratégies du rôle.

Exemple de délégation

Vous pouvez créer un rôle avec des règles pour un membre ou administrateur. Puis, vous pouvez affecter le rôle de sorte que d'autres utilisateurs, non encore conformes aux règles, puissent devenir membre avec rôle ou administrateur de rôles.

Examinez l'exemple suivant, décrivant des administrateurs qui gèrent les droits d'application métier des utilisateurs finals :

- Jeff est propriétaire du rôle de comptable ; par conséquent, lorsque ce rôle requiert des modifications, Jeff le modifie.
- David et Lisa sont des administrateurs de ce rôle. Ils affectent des utilisateurs régionaux comme membres avec rôle.
- D'autres utilisateurs sont membres avec rôle sans être affectés en tant que tels. En revanche, ils satisfont la règle pour être membres avec rôle.

  Les membres avec rôle utilisent le rôle de comptable pour générer des bons de commande et effectuer d'autres tâches dans des applications financières.

La section Caractéristiques de rôles fournit des détails sur les règles et ainsi que d'autres caractéristiques d'un rôle.

Caractéristiques des rôles

Lorsque vous créez un rôle, vous définissez les caractéristiques affichées dans le tableau suivant :

Caractéristiques	Définition
Profil du rôle	Caractéristiques générales du rôle
Tâches	Tâches pour un rôle d'administration
Modèles de compte	Modèles définissant les comptes sur des terminaux gérés pour un rôle de provisionnement
Règles de membre Stratégies de membre	Une règle de membre définit les conditions permettant à un utilisateur d'être membre du rôle d'administration ou d'accès. Une stratégie de membre combine une règle de membre et des règles de portée. **Remarque :** Les rôles de provisionnement n'incluent pas de règles de membre et de stratégies. Pour qu'un utilisateur devienne membre, utilisez Modifier les membres/administrateurs avec rôle de provisionnement.

Caractéristiques	Définition
Règles d'administration Stratégies d'administration	■ Une règle d'administration définit les conditions permettant à un utilisateur de devenir administrateur de rôles. ■ Une stratégie d'administration combine une règle d'administration et une règle de portée et des droits d'administrateur pour affecter le rôle.
Règles de propriété	Conditions permettant à un utilisateur de devenir propriétaire d'un rôle
Règles de portée	Limites des objets pouvant être gérés par le rôle
Actions Ajouter Actions Supprimer	Modifications apportées à un profil d'utilisateur lorsqu'un utilisateur est ajouté ou supprimé en tant que membre du rôle.

Profil du rôle

Le profil du rôle représente le nom et la description du rôle et indique si celui-ci est activé ou non. S'il est activé, le rôle pourra être utilisé dès sa création.

Tâches du rôle

Dans le cas d'un rôle d'administration, vous pouvez choisir une ou plusieurs tâches d'administration, y compris des tâches externes, à partir d'une ou plusieurs catégories.

Modèles de compte

Chaque rôle de provisionnement contient des modèles de compte. Ceux-ci définissent les comptes qui existent dans des terminaux gérés. Par exemple, le terminal d'un compte Exchange peut définir la taille de la boîte aux lettres. Ces modèles de compte définissent également la manière dont les attributs d'utilisateurs sont mappés vers les comptes.

Vous pouvez choisir un ou plusieurs terminaux pour chaque type de terminal. Un utilisateur auquel le rôle est affecté reçoit un compte dans le terminal.

Règles de membre, d'administration et de propriété

Chaque rôle inclut des règles déterminant qui peut être membre, administrateur ou propriétaire de ce rôle. Par conséquent, un utilisateur pourrait être membre d'un rôle, de plusieurs ou d'aucun.

Les règles de membre, d'administration et de propriété utilisent les conditions du tableau ci-après.

Condition des règles	Exemple	Syntaxe des règles
L'utilisateur doit correspondre à une valeur d'attribut.	Utilisateurs dont le titre commence par "senior"	où <filtre-utilisateur>
L'utilisateur doit correspondre à plusieurs valeurs d'attribut.	Utilisateurs dont titre=gestionnaire et localité=est	où <filtre-utilisateur>
L'utilisateur doit appartenir à des organisations nommées.	Utilisateurs dans le service commercial de l'organisation et niveau inférieur	dans <règle-org>
L'utilisateur doit appartenir aux organisations qui sont conformes à une condition spécifiée par les attributs de l'organisation.	Utilisateurs dans les organisations où type d'activité=or ou platine	dans les organisations où <filtre-org>
L'utilisateur doit appartenir à des organisations spécifiques et correspondre à des attributs d'utilisateur spécifiques.	Utilisateurs dont titre=gestionnaire et localité=est et qui sont dans le service commercial ou marketing de l'organisation	où <filtre-utilisateur> et figurant dans <règle-org>
L'utilisateur doit appartenir à un groupe spécifique.	Utilisateurs qui sont membres du groupe 401K	membres du groupe <groupe>
L'utilisateur doit être membre d'un rôle.	Utilisateurs qui sont membres du rôle Centre d'assistance	membres de <règle-rôle>
L'utilisateur doit être administrateur d'un rôle.	Utilisateurs qui sont administrateurs du rôle Gestionnaire des ventes	qui sont administrateurs de <règle-rôle>
L'utilisateur doit être propriétaire d'un rôle.	Utilisateurs qui sont propriétaires du rôle Gestionnaire d'utilisateurs	qui sont propriétaires de <règle-rôle>
L'utilisateur doit appartenir à un groupe qui satisfait à une condition spécifiée par les attributs du groupe.	Utilisateurs qui sont membres des groupes où propriétaire=PDG	membres du groupe <filtre-groupe>

Condition des règles	Exemple	Syntaxe des règles
L'utilisateur doit satisfaire à une condition basée sur une requête LDAP.	Utilisez un annuaire LDAP dans les cas où une requête créée dans la console d'utilisateur Identity Manager n'est pas suffisante.	utilisateur renvoyé par la requête requête_LDAP

Certaines règles peuvent impliquer la comparaison d'une valeur avec un attribut à valeurs multiples. Pour que la règle s'applique, au moins une valeur de cet attribut doit satisfaire à la règle. Par exemple, si la règle est Attribut A EGAL A 1 et que la valeur de l'attribut A est 1, 2 ou 3 pour l'utilisateur X, alors l'utilisateur X remplit les critères.

Il se peut que l'utilisateur qui crée le rôle ne puisse pas le modifier. Pour pouvoir l'éditer, cet utilisateur doit répondre aux conditions des règles de propriété.

Remarque : Dans les implémentations à grande échelle, l'évaluation des règles de membre, d'administration et de propriété peut prendre beaucoup de temps. Pour réduire le temps d'évaluation des règles comprenant des attributs d'utilisateur, vous pouvez activer l'option d'évaluation en mémoire. Pour plus d'informations, consultez le *Manuel de configuration*.

Règles de portée

Vous associez des règles de membre et d'administration aux règles de portée. Les *règles de portée* limitent les objets pour lesquels le rôle peut être utilisé.

- Pour un membre du rôle, les règles de portée contrôlent quels objets peuvent être gérés dans le rôle.
- Pour un administrateur du rôle, les règles de portée contrôlent quels utilisateurs peuvent devenir membres ou administrateurs du rôle.

Les objets incluent l'objet principal de la tâche et tous les objets secondaires. Par exemple, une tâche de création d'utilisateur incluant un onglet Groupe a un objet principal d'utilisateur et un objet secondaire de groupe.

Pour la plupart des types d'objets, vous pouvez spécifier les types de règles de portée dans la table suivante.

Condition des règles	Exemple	Syntaxe des règles
Tous	Les membres du rôle peuvent gérer tous les objets	Tous
L'objet doit correspondre à une ou plusieurs valeurs d'attributs.	Utilisateurs où le **titre** commence par **senior**	où <filtre>

Quand vous sélectionnez l'option Filtre, CA IdentityMinder affiche deux types de filtres :

<attribut><comparateur><valeur>

Un attribut dans le profil de l'objet doit correspondre à la valeur spécifiée.

<attribut> <comparateur> <attribut-utilisateur> d'administrateur

Un attribut dans le profil de l'objet doit correspondre à un attribut dans le profil de l'administrateur. Par exemple : utilisateurs où gestionnaire = ID utilisateur de l'administrateur.

Des options supplémentaires, qui sont décrites dans les tables suivantes, sont disponibles pour les objets utilisateurs, groupes et organisations.

Remarque Les règles de portée d'utilisateur suivantes sont des exemples. Vous pouvez créer d'autres règles pour traiter les différentes relations entre l'administrateur et les utilisateurs que l'administrateur peut gérer.

Condition des règles	Exemple	Syntaxe des règles
L'utilisateur doit correspondre à une valeur d'attribut.	Utilisateurs où un membre d'un groupe commercial ou téléphone portable n'est pas égal à nul	où <filtre-utilisateur>
L'utilisateur doit correspondre à plusieurs valeurs d'attribut.	Utilisateurs où titre=gestionnaire et localité=USA	où <filtre-utilisateur>
L'utilisateur doit appartenir à des organisations nommées.	Utilisateurs dans l'organisation Australie ou Nouvelle Zélande **Remarque :** La règle de portée de l'organisation s'applique aux sous-organisations de l'organisation qui est conforme à la règle. Par exemple, si la règle de l'organisation est "dans Organisation1", la règle de portée s'applique à Organisation1.1 et Organisation1.2, mais pas à Organisation1.	dans <règle-org>
L'utilisateur doit appartenir aux organisations qui sont conformes à une condition spécifiée par les attributs sur l'organisation.	Utilisateurs dans les organisations où type d'activité=or ou platine	dans les organisations où <filtre-org>

Condition des règles	Exemple	Syntaxe des règles
L'utilisateur doit appartenir à des organisations spécifiques et correspondre à des attributs d'utilisateur spécifiques.	Utilisateurs où titre=gestionnaire et localité=est et qui sont dans le service commercial ou marketing de l'organisation	où <filtre-utilisateur> et qui sont dans <règle-org>
L'attribut dans un profil d'utilisateur doit correspondre à un attribut dans le profil de l'administrateur.	Utilisateurs où gestionnaire = ID utilisateur de l'administrateur.	où <attribut-utilisateur> <comparateur> <attribut-utilisateur> de l'administrateur **Remarque :** N'utilisez que le comparateur Différent de avec un attribut à valeurs multiples.
L'utilisateur est dans la même organisation que l'administrateur.	Utilisateurs dans l'organisation dont Jeff (l'administrateur) est membre	organisation de l'administrateur
L'utilisateur est dans une organisation qui est répertoriée dans l'attribut de l'administrateur.	Utilisateurs dans secteur commercial ou marketing	organisation qui est une valeur dans <attribut-admin> de l'administrateur

Remarque Les règles de portée de groupe suivantes sont uniquement des exemples. Vous pouvez créer d'autres règles pour traiter les différentes relations entre l'administrateur et les groupes que l'administrateur peut gérer.

Condition des règles	Exemple	Syntaxe des règles
Le groupe doit correspondre à une valeur d'attribut.	Nom de groupe où nom de groupe = 401K	où <filtre-groupe>
Les groupes doivent appartenir à des organisations nommées.	Groupes dans comptabilité de l'organisation et moins que	dans <règle-org>
Le groupe doit correspondre à une valeur d'attribut et appartenir à des organisations nommées.	Groupes où Type d'activité = finance et qui sont dans le secteur commercial de l'organisation et moins que	où <filtre-groupe> et qui sont dans <règle-org>

Condition des règles	Exemple	Syntaxe des règles
Le groupe doit être répertorié dans un attribut de l'administrateur.	Groupes où Description = Ingénierie	où <attribut-groupe> <comparateur> <attribut-utilisateur> de l'administrateur **Remarque :** N'utilisez que le comparateur Différent de avec un attribut à valeurs multiples.

Remarque Les règles de portée d'organisation suivantes sont uniquement des exemples. Vous pouvez créer d'autres règles pour traiter les différentes relations entre l'administrateur et les organisations que l'administrateur peut gérer.

Condition des règles	Exemple	Syntaxe des règles
L'organisation doit correspondre à une valeur d'attribut.	organisations où Nom org =finance	où <filtre-org>
Les organisations doivent appartenir à des organisations nommées.	organisations dans finance et moins que	dans <règle-org>
L'organisation doit correspondre à une valeur d'attribut et appartenir à une organisation nommée.	organisations où Nom org =finance et sont en finance et moins que	où <filtre-org> et sont dans <filtre-org>

Informations complémentaires :

Directives générales concernant les règles (page 28)

Directives générales concernant les règles

Quel que soit le type de règle créée, il importe de comprendre comment Identity Manager les traite.

Evaluation d'opérateurs

Lors de la création de règles pour un rôle, vous pouvez inclure les opérateurs >=, <=, < et >. Toutefois, ces opérateurs sont considérés comme des chaînes par l'annuaire LDAP ou la base de données relationnelles. La plupart des référentiels d'utilisateurs effectuent des comparaisons de chaînes en fonction de leur alphabet. Par conséquent, en comparant 500 et 1100, le référentiel d'utilisateurs peut déterminer que 500 est supérieur, car 5 est supérieur à 1.

Vous pouvez modifier la méthode de comparaison des chaînes dans le référentiel d'utilisateurs. Consultez la documentation du service d'annuaire LDAP ou le logiciel de base de données relationnelles.

Non-respect de la casse dans les règles

Lors de la création de rôles d'administration ou d'accès, les règles que vous créez peuvent être évaluées en tenant compte ou non de la casse, selon le référentiel d'utilisateurs.

Toutefois, à l'issue d'une opération de création ou de modification, les règles sont évaluées en interne sans tenir compte de la casse avant l'application des modifications au référentiel d'utilisateurs. Par exemple, si une règle possède une condition dans laquelle titre=gestionnaire, cette règle correspondra à l'objet de référentiel d'utilisateurs, que la valeur de son titre soit gestionnaire ou Gestionnaire.

Actions Ajouter et Supprimer

Vous devez spécifier une action d'ajout et de suppression pour qu'Identity Manager puisse gérer correctement l'appartenance à un rôle lorsqu'un administrateur accorde ou révoque le rôle.

- L'action d'ajout doit permettre d'associer l'utilisateur aux critères dans l'une des règles de membre du rôle. Par exemple, si la règle de membre pour le rôle de gestionnaire d'utilisateurs indique que la valeur de l'attribut Rôles d'administration des membres avec rôle est Gestionnaire d'utilisateurs, l'action Ajouter devra ajouter Gestionnaire d'utilisateurs à l'attribut Rôles d'administration.
- De même, l'action Supprimer doit modifier le profil d'un utilisateur afin qu'il ne corresponde plus à la règle de membre lorsque celle-ci est retirée.

Chaque rôle peut comprendre deux *actions Ajouter* et deux *actions Supprimer*.

Si les administrateurs peuvent ajouter et supprimer des membres avec rôle, définissez des actions Ajouter et Supprimer. Sinon, l'utilisateur disposera du rôle s'il correspond à la règle de membre, par exemple en appartenant au groupe RoleAdmins. Exemple :

- Le rôle A peut être affecté par un administrateur ; les actions Ajouter ou Supprimer seront donc définies.
- Le rôle B contient une règle indiquant que tous les membres du groupe Finances disposent du rôle. Ce rôle ne peut pas être affecté ; il ne contient donc aucune action Ajouter ou Supprimer.

Lors de la définition des actions Ajouter et Supprimer, envisagez d'utiliser l'attribut Rôle d'administration, que CA Identity Manager peut utiliser pour stocker une liste de rôles d'utilisateurs. Par exemple, vous pouvez configurer une action Ajouter pour ajoute Employé à l'attribut Rôle d'administration d'un utilisateur lorsque ce dernier est ajouté comme membre du rôle Employé. Si un administrateur affecte le rôle Employé à un gestionnaire qui dispose déjà des rôles Auto-administrateur et Gestionnaire d'utilisateurs, l'attribut Rôle d'administration du gestionnaire contiendra les valeurs suivantes : Self Administrator, User Manager, Employee.

Pour utiliser l'attribut Rôle d'administration, l'attribut connu %ADMIN_ROLE_CONSTRAINT% doit être mappé vers un attribut à valeurs multiples dans des profils d'utilisateur. Pour plus d'informations, consultez le *Manuel de configuration de CA Identity Manager*.

Important : Lors de la définition d'une action Ajouter, évitez de configurer une règle faisant référence au rôle que vous définissez. Par exemple, ne définissez pas d'action Ajouter qui établit un membre du Rôle A en étant un membre du Rôle A. Cela provoquera une erreur récursive qui entraînera le redémarrage du serveur de stratégies.

Stratégies de membre

Une *stratégie de membre* indique que si un utilisateur correspond à la règle de membre, sa portée sera définie dans cette stratégie. Le graphique suivant illustre un rôle comprenant deux stratégies de membre.

- La première stratégie indique que si un membre avec rôle dispose du gestionnaire Jones, ce membre peut utiliser le rôle avec des utilisateurs du service Ventes et les gérer en tant que membres du groupe 401k.

- La deuxième stratégie indique que si un membre avec rôle se trouve dans la ville de Bend, il peut utiliser le rôle avec des utilisateurs dans l'état de l'Oregon et les gérer en tant que membres des groupes dont l'administrateur est Smith.

Member Policies

	Member Rule	User Scope Rule	Group Scope Rule
	where (Manager = "Jones")	where (Office = "Sales")	where (Group Name = "401K")
	where (City = "Bend")	where (State = "OR")	where (Group Admin = "Smith")

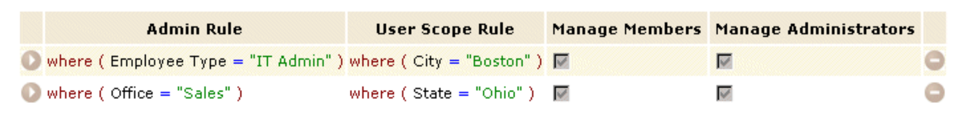
Stratégies d'administration

Une *stratégie d'administration* indique que si un utilisateur correspond à la règle d'administration, sa portée et ses droits d'administrateur seront définis dans cette stratégie. La portée de l'utilisateur définit l'emplacement de l'utilisation du rôle. Les droits d'administrateur déterminent si l'administrateur de rôles peut gérer des membres ou des administrateurs du rôle.

Le graphique suivant illustre un rôle contenant deux stratégies d'administration, définies comme suit :

- Dans le cas de la première stratégie, un administrateur informatique peut ajouter et supprimer des membres avec rôle et des administrateurs de rôles aux utilisateurs situés dans la ville de Boston.
- Dans le cas de la deuxième stratégie, un administrateur du service Ventes peut ajouter et supprimer des membres dans l'état de l'Ohio.

Admin Policies



	Admin Rule	User Scope Rule	Manage Members	Manage Administrators	
	where (Employee Type = "IT Admin")	where (City = "Boston")	☑	☑	
	where (Office = "Sales")	where (State = "Ohio")	☑	☑	

Liste de contrôle de planification des rôles

Avant de créer un rôle, utilisez cette liste de contrôle de caractéristiques de rôles.

Caractéristique de rôles	Détails
Profil du rôle	Définissez un nom et une description pour le rôle et définissez le statut sur Activé.
Tâches	Incluez des tâches d'administration ou d'accès.
Modèles de compte	Incluez des modèles de compte qui définissent des comptes présents dans des terminaux (rôles de provisionnement uniquement).
Stratégies de membre	Pour chaque stratégie de membre, définissez les éléments suivants : ■ Règles de membre : utilisateurs du rôle ■ Règles de portée : objets pouvant être gérés par un membre avec rôle ■ Action Ajouter : événements qui s'appliquent au profil d'un utilisateur qui devient membre ■ Action Supprimer : événements qui s'appliquent au profil d'un utilisateur supprimé comme membre
Stratégies d'administration	Pour chaque stratégie d'administration : ■ Règles d'administration : personnes pouvant gérer les utilisateurs comme membres ou administrateurs ■ Règles de portée : utilisateurs que l'administrateur peut gérer comme membres ou administrateurs ■ Action Ajouter : événements qui s'appliquent au profil d'un utilisateur qui devient administrateur ■ Action Supprimer : événements qui s'appliquent au profil d'un utilisateur supprimé comme administrateur
Règles de propriété	Définissez les utilisateurs pouvant modifier le rôle.

Chapitre 2: Rôles d'administration

Ce chapitre traite des sujets suivants :

Rôles d'administration et tâches d'administration

Vous pouvez créer des rôles contenant des tâches de gestion d'objets en fonction des besoins de votre entreprise. Vous pouvez par exemple créer des rôles contenant des tâches de gestion des utilisateurs et des rôles contenant des tâches de gestion des rôles créés.

Vous pouvez également créer différents rôles grâce aux tâches suivantes :

- Tâches permettant aux administrateurs de gérer les utilisateurs
- Tâches de gestion des administrateurs
- Tâches de gestion des rôles d'administration
- Tâches de gestion des rôles d'accès

Remarque : Vous pouvez également utiliser les rôles d'administration par défaut fournis avec CA IdentityMinder. Ces rôles comportent des tâches regroupées dans des catégories similaires à la liste précédente.

Rôles d'administration et environnements Identity Manager

Lorsque vous vous connectez à un environnement Identity Manager, votre compte d'utilisateur comporte un ou plusieurs rôles d'administration. Chaque rôle d'administration contient des tâches (par exemple, Créer un utilisateur) que vous utilisez dans cet environnement Identity Manager.

Par exemple, dans l'environnement Identity Manager *central*, un rôle d'administration, de *Centre d'assistance*, contient des tâches de réinitialisation de mots de passe. Le rôle comporte une règle de membre selon laquelle l'utilisateur doit être un employé du service informatique. Lorsque des employés du service informatique se connectent à l'environnement Identity Manager *central*, ils disposent du rôle *Centre d'assistance* et peuvent réinitialiser les mots de passe des utilisateurs figurant dans cet environnement Identity Manager.

Rôles d'administration et console d'utilisateur

Un environnement Identity Manager s'affiche via la console d'utilisateur. Les rôles d'administration qui vous sont affectés déterminent les éléments qui s'affichent dans cette console, comme indiqué dans le tableau suivant :

Rôles affectés	Format de la console d'utilisateur
Rôle Gestionnaire de systèmes	Liste de catégories de tous les objets et de toutes les tâches d'administration par défaut permettant de gérer ces objets
Rôles permettant de gérer plusieurs types d'objets	Liste de catégories accompagnée d'un élément pour chaque type d'objet que vous pouvez gérer
Rôles permettant de gérer un type d'objet (par exemple, Utilisateurs)	Tâches correspondant à cet objet (par exemple, Modifier un utilisateur) *sans* liste de catégories
Rôle d'approbation	Liste de travail Cette fenêtre apparaît si certaines tâches de l'administrateur sont en attente d'approbation (par exemple, approbation de l'auto-enregistrement d'utilisateurs).

Si vous pouvez gérer plusieurs objets, la liste de catégories affiche les objets que vous pouvez modifier (par exemple, Utilisateurs et Groupes) sous forme d'onglets répartis dans la partie supérieure de la fenêtre. Sélectionnez un onglet pour afficher les tâches associées aux rôles qui vous sont affectés.

Remarque : Si votre navigateur Internet ne prend pas en charge les feuilles de styles en cascade, la console d'utilisateur utilise un format différent. Pour contrôler ce format, reportez-vous au *Manuel de configuration*.

Création d'un rôle d'administration

Une fois les besoins liés au rôle connus, vous pouvez créer un rôle d'administration. Ces besoins concernent l'utilisateur de ce rôle, les objets gérés par ce rôle et l'environnement contenant les objets à gérer.

Création initiale d'un rôle d'administration

Un rôle d'administration se crée via la console d'utilisateur.

Pour créer un rôle d'administration :

1. Connectez-vous à un compte CA IdentityMinder qui comporte un rôle contenant des tâches de création de rôles d'administration.

   Par exemple, le premier utilisateur d'un environnement dispose du rôle Gestionnaire de systèmes, qui comporte la tâche Créer un rôle d'administration.

2. Sous Rôles et tâches, sélectionnez Rôles d'administration, puis Créer un rôle d'administration.

3. Choisissez l'option de création de rôle ou de copie d'un rôle.

   L'onglet Profil apparaît : vous pouvez commencer à y définir le rôle d'administration.

4. Définissez le profil du rôle d'administration.

Définition du profil du rôle d'administration

L'onglet Profil permet de définir les caractéristiques de base du rôle.

Pour définir le profil :

1. Entrez un nom et une description, puis spécifiez les autres attributs personnalisés définis pour le rôle.

   Remarque : Dans l'onglet Profil, vous pouvez spécifier des attributs personnalisés qui indiquent des informations supplémentaires sur les rôles d'accès. Vous pouvez utiliser ces dernières pour faciliter les recherches de rôles dans les environnements comprenant un nombre important de rôles.

2. Sélectionnez Activé si le rôle peut être mis à la disposition des utilisateurs dès qu'il est créé.

3. Sélectionnez des tâches d'administration pour le rôle (page 36).

Informations complémentaires :

Attributs personnalisés définis par l'utilisateur pour les rôles (page 53)

Sélection de tâches d'administration pour le rôle

L'onglet Tâches permet de sélectionner les tâches d'administration à inclure dans le rôle. Vous pouvez inclure des tâches issues de différentes catégories ou copier des tâches utilisées dans un autre rôle.

Pour sélectionner des tâches d'administration :

1. Sélectionnez la catégorie dans le champ Filtrer par catégorie.

   Pour afficher la liste des catégories de tâche disponibles, cliquez sur l'icône représentant une flèche vers le bas.

2. Sélectionnez la tâche à inclure dans le rôle dans le champ Ajouter une tâche.

   CA IdentityMinder ajoute la tâche à la liste des tâches dans le rôle.

3. Ajoutez des tâches supplémentaires en répétant les étapes 1 et 2.
4. Supprimez une tâche du rôle en cliquant sur l'icône représentant un signe moins ( ) pour cette tâche.
5. Définissez des stratégies de membres pour un rôle d'administration (page 37).

Définition de stratégies de membres pour un rôle d'administration

L'onglet Membres permet de créer des stratégies de membres et de déterminer quels utilisateurs peuvent être membres de rôles.

Pour définir des stratégies de membres :

1. Pour définir des stratégies de membres, cliquez sur Ajouter. Une stratégie de membre comporte les règles suivantes :

   - Une règle de membre qui définit les conditions requises pour qu'un utilisateur soit membre d'un rôle.

     Remarque : Les opérateurs suivants traitent les nombres comme des caractères dans les règles de membres :

     - Inférieur à (<)
     - inférieur ou égal à (<=)
     - Supérieur à (>)
     - Supérieur ou égal à (=>)

     Par exemple, "10" vient après "1" mais avant "2".

   - Des règles de portée qui limitent les objets principal et secondaire accessibles aux tâches figurant dans le rôle.

     Par exemple, si le rôle comporte une tâche qui permet de modifier les utilisateurs en les affectant à des groupes, la règle de portée d'utilisateur limite les utilisateurs (objet principal) pouvant être trouvés et la règle de portée de groupe limite les groupes (objet secondaire) pouvant être affectés.

   Remarque : Assurez-vous de répondre à au moins une question de portée. Les règles de portée limitent les objets principal et secondaire accessibles aux tâches figurant dans le rôle. Par exemple, si le rôle comporte une tâche qui modifie les utilisateurs en les affectant à des groupes, la règle de portée d'utilisateur limite les utilisateurs (objet principal) pouvant être trouvés et la règle de portée de groupe les groupes (objet secondaire) pouvant être affectés.

2. Vérifiez que la stratégie de membre apparaît dans l'onglet Membres.

   - Pour modifier une stratégie, cliquez sur la flèche vers la droite située à gauche.
   - Pour la supprimer, cliquez sur l'icône représentant un signe moins.

3. Dans l'onglet Membres, activez la case à cocher Les administrateurs peuvent ajouter et supprimer des membres à ce rôle, sauf si les utilisateurs peuvent devenir membres grâce à une seule règle de membre.

   Une fois cette fonctionnalité activée, la fenêtre se développe.

4. Dans la zone développée, définissez les actions Ajouter et Supprimer pour les cas où un utilisateur est ajouté ou supprimé en tant que membre de rôle.

   Important : Lorsque vous définissez une action Ajouter, évitez de définir une règle se référant au rôle en cours de définition. Par exemple, afin d'éviter toute erreur, un utilisateur ne doit pas définir l'action Ajouter pour créer un membre du rôle A s'il est lui-même membre de ce rôle.

5. Définissez de stratégies d'administration pour un rôle d'administration (page 38).

Définition de stratégies d'administration pour un rôle d'administration

L'onglet Administrateurs permet de définir quelles personnes peuvent ajouter ou supprimer des utilisateurs en tant que membres et administrateurs de ce rôle.

Pour définir des stratégies d'administration :

1. Si vous souhaitez que l'option Gérer les administrateurs soit disponible, cochez la case Les administrateurs peuvent ajouter des administrateurs à ce rôle et les en supprimer.

   Une fois cette fonctionnalité activée, la fenêtre se développe.

2. Dans la zone développée, définissez les actions Ajouter et Supprimer pour les cas où un utilisateur est ajouté ou supprimé en tant qu'administrateur du rôle.

3. Définissez des stratégies d'administration, qui comportent des règles de portée et d'administration et au moins un droit d'administrateur (Gérer les membres ou Gérer les administrateurs).

   Remarque : Vous pouvez ajouter plusieurs stratégies d'administration comportant différentes règles et différents droits pour les administrateurs qui observent la règle.

4. Pour modifier une stratégie, cliquez sur la flèche située à gauche. Pour la supprimer, cliquez sur l'icône représentant un signe moins.

5. Définissez des règles de propriété pour un rôle d'administration (page 39).

Définition de règles de propriété pour un rôle d'administration

L'onglet Propriétaires permet de définir des règles déterminant quels utilisateurs peuvent être propriétaires d'un rôle et ceux autorisés à modifier ce rôle.

Pour définir des règles de propriété :

1. Pour déterminer quels utilisateurs sont autorisés à modifier le rôle, définissez des règles de propriété.
2. Cliquez sur Soumettre.

   Un message s'affiche indiquant que la tâche a été soumise. Un léger retard peut se produire avant qu'un utilisateur puisse utiliser le rôle.

Si vous avez sélectionné Activé lors de la création du rôle, le rôle est disponible et peut être utilisé. Si un utilisateur remplit les conditions de la règle de membre, il peut à présent se connecter à l'environnement Identity Manager et utiliser les tâches figurant dans le rôle.

Vérification d'un rôle d'administration

Pour vérifier que le rôle a été créé, choisissez Rôles d'administration, puis Afficher un rôle d'administration, et sélectionnez le nom du rôle.

Pour vérifier que la tâche de création de rôle est terminée, vous pouvez également choisir Système, puis Afficher les tâches soumises.

Autorisation donnée aux utilisateurs pour l'auto-affectation de rôles

Un environnement peut contenir certains rôles que les utilisateurs peuvent s'affecter. Vous pouvez, par exemple, autoriser des utilisateurs à s'inscrire au rôle Gestionnaire de délégations afin qu'ils puissent déléguer les tâches d'un utilisateur à un autre utilisateur.

Pour déterminer les rôles que les utilisateurs peuvent s'affecter, configurez des critères dans la tâche Auto-gestionnaire des rôles.

Pour autoriser les utilisateurs à s'affecter des rôles :

1. Modifiez la tâche Auto-gestionnaire des rôles comme suit :
   a. Sélectionnez Rôles et tâches, puis Modifier la tâche d'administration et recherchez la tâche Auto-gestionnaire des rôles.
   b. Cliquez sur l'onglet Onglets.

      CA IdentityMinder affiche la liste des onglets qui s'appliquent à la tâche.

c. Pour modifier cette tâche, sélectionnez l'icône flèche droite située en regard de l'onglet Auto-gestionnaire des rôles.

d. Complétez les champs suivants :

Afficher uniquement les rôles d'administration correspondant aux règles suivantes

Spécifie les critères qu'utilise CA IdentityMinder pour déterminer les rôles que les utilisateurs sont autorisés à s'affecter.

Pour ajouter des règles supplémentaires, cliquez sur l'icône plus (+).

Utilisateur servant d'administrateur du rôle d'administration

Spécifie l'administrateur pour les rôles que les utilisateurs peuvent s'affecter.

Pour les rôles que les utilisateurs peuvent s'affecter, l'utilisateur doit être sélectionné en tant qu'administrateur dans ce champ *et* correspondre aux critères spécifiés dans le champ Afficher uniquement les rôles d'administration correspondant aux règles suivantes.

Fenêtre de liste

Spécifie les colonnes et le format pour la liste des rôles qu'un utilisateur peut sélectionner pour s'affecter un rôle.

e. Cliquez sur OK, puis sur Soumettre.

2. Ajoutez la tâche Auto-gestionnaire des rôles à un rôle, puis affectez ce rôle aux utilisateurs devant pouvoir effectuer cette tâche.

Chapitre 3: Tâches d'administration

Ce chapitre traite des sujets suivants :

Planification de tâches d'administration

Les rôles d'administration comprennent plusieurs tâches d'administration, qui permettent de gérer des objets avec précision. Par exemple, vous pouvez gérer un objet Utilisateurs à l'aide des tâches d'administration suivantes :

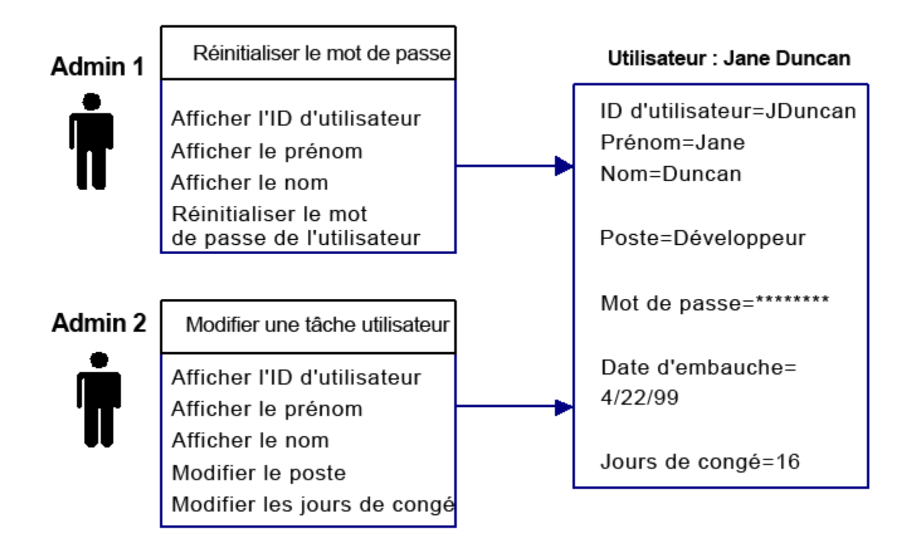
- Créer un utilisateur
- Afficher un utilisateur
- Modifier un utilisateur
- Réinitialiser le mot de passe de l'utilisateur

Créez ou modifiez chaque tâche en fonction de vos propres besoins. Ensuite, combinez les tâches d'administration appropriées dans des rôles d'administration, que vous affectez à des administrateurs. Avec ces rôles, les administrateurs disposent exactement des droits dont ils ont besoin pour gérer les objets.

Pour planifier la création de tâches d'administration, choisissez les objets à gérer (Utilisateurs, Groupes, Organisations, Rôles ou Tâches) ainsi que les administrateurs qui utiliseront ces tâches. Par exemple :

- Pour gérer les utilisateurs, les administrateurs du centre d'assistance nécessitent des tâches qui gèrent les attributs d'utilisateurs (par exemple, un ID d'utilisateur ou un titre).
- Pour gérer l'accès des utilisateurs aux applications, les autres administrateurs nécessitent des tâches permettant de convertir ces utilisateurs en membres des rôles d'accès.
- Pour gérer les rôles utilisés par les administrateurs du centre d'assistance, les administrateurs de niveau supérieur nécessitent des tâches qui gèrent les rôles d'administration.

Pour un type d'objet (par exemple, Utilisateurs), vous pouvez créer des tâches de sorte que différents administrateurs gèrent différents attributs. Par exemple, le schéma suivant présente un utilisateur géré par deux administrateurs.



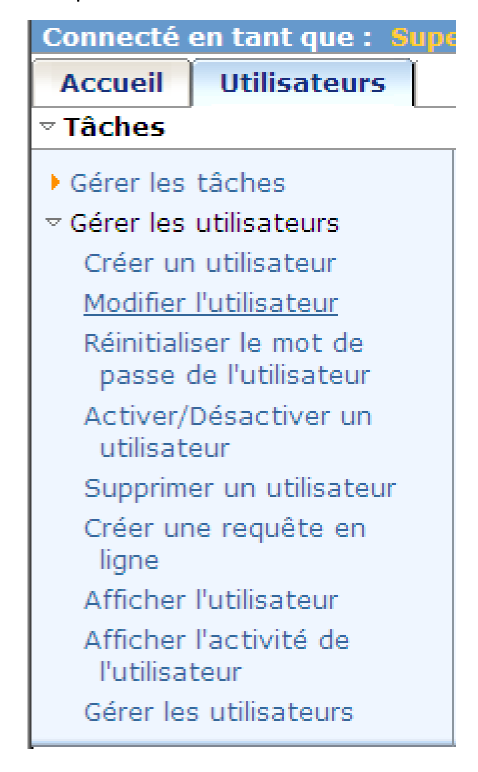
- Admin 1 dispose de la tâche Réinitialiser le mot de passe de l'utilisateur ; cet administrateur peut voir l'ID d'utilisateur et le nom de l'employé ou réinitialiser son mot de passe.
- Admin 2 dispose de la tâche Modifier un utilisateur ; cet administrateur peut voir l'ID d'utilisateur et le nom de l'employé ou modifier son titre et ses jours de congé.

Exemple de tâche d'administration

Lorsque vous créez une tâche d'administration, vous définissez le contenu et la présentation de ses fenêtres, notamment les éléments ci-après.

- Le nom de la tâche
- La catégorie contenant la tâche
- Les onglets et les champs à utiliser dans la tâche, ainsi que les propriétés d'affichage des champs
- Les champs qu'un administrateur peut utiliser dans une requête de recherche, ainsi que les champs affichés dans les résultats de recherche

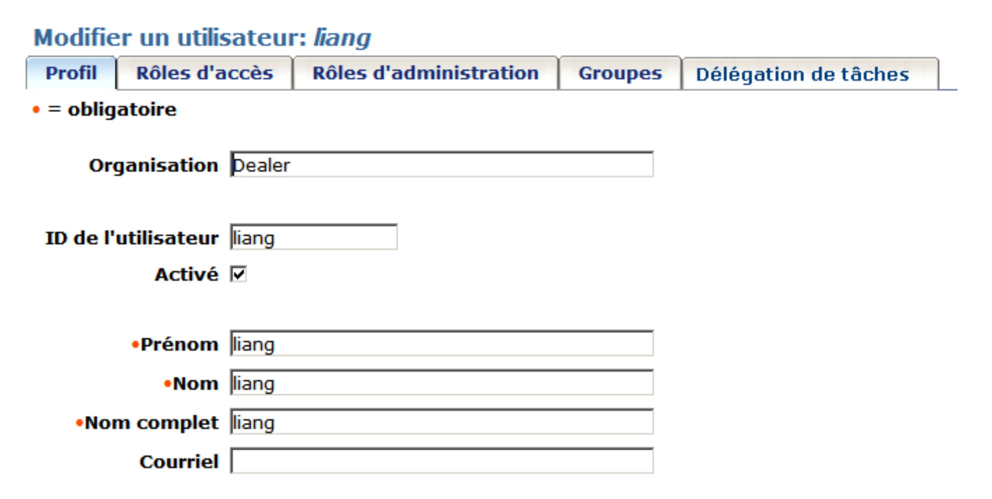
Pour comprendre les éléments d'une tâche, examinons la tâche Modifier l'utilisateur. Dans ce cas, Utilisateurs est la catégorie, Gérer les utilisateurs est une sous-catégorie et Modifier l'utilisateur est la tâche. Les noms de la catégorie et de la tâche sont créés lorsque vous créez une tâche.



Lorsque vous choisissez Modifier l'utilisateur, une fenêtre de recherche s'affiche. Une *fenêtre de recherche* fournit des options permettant de rechercher l'objet à afficher ou à modifier. Chaque option est nommée *filtre*, une limite qui s'applique aux objets trouvés par la recherche.

Une fois la fenêtre de recherche remplie, une fenêtre à onglets s'affiche. Par exemple, la figure suivante affiche les onglets correspondant à la tâche Modifier l'utilisateur. L'onglet Profil apparaît en premier et affiche les attributs de l'utilisateur, tandis que les autres onglets affichent les droits de rôle et de groupe de l'utilisateur.

Pour la tâche que vous créez, choisissez les onglets à inclure et déterminez l'ordre et le contenu.



Par exemple, en utilisant la tâche Modifier l'utilisateur comme modèle, vous pouvez créer une tâche Modifier un sous-traitant, qui modifie les éléments ci-après.

- Champs figurant dans l'onglet Profil
- Onglets à inclure dans la tâche et leur contenu
- Catégorie dans laquelle la tâche s'affiche

  Vous pouvez créer cette tâche dans une nouvelle catégorie, Sous-traitant.

La tâche Modifier un sous-traitant inclut certains des champs figurant dans l'onglet Profil de la tâche Modifier l'utilisateur, ainsi que d'autres champs, tels que la date de début du contrat et l'entreprise du sous-traitant. Les administrateurs peuvent rechercher un sous-traitant en fonction de son nom, de son entreprise et de la date de début.

Modify Contractor: *jhansen*

Profile | Groups | Contractor Roles

User ID jhansen

Enabled

First Name Julia

Last Name Hansen

Email jhansen@wxyz.com

Start Date 10/19/2007

Company

La nouvelle tâche comporte également un onglet Rôles des sous-traitants, où vous pouvez ajouter des rôles aux sous-traitants.

Options d'utilisation des tâches d'administration

Identity Manager permet d'utiliser les tâches d'administration de deux manières.

- **Sélection de la tâche**

  Vous sélectionnez une catégorie et une tâche, puis recherchez l'objet auquel la tâche s'applique.

  Par exemple, pour modifier un profil d'utilisateur, sélectionnez la catégorie Utilisateurs, puis la tâche Modifier l'utilisateur. Recherchez ensuite l'utilisateur à modifier.

- **Sélection de l'objet**

  Vous utilisez les tâches de gestion (par exemple, Gérer les utilisateurs ou Gérer les groupes) pour rechercher un objet. Une fois l'objet sélectionné, vous pouvez afficher une liste de tâches que vous pouvez utiliser pour gérer cet objet. Cette méthode est appelée *navigation objet/tâche.*

  Par exemple, pour modifier un utilisateur à l'aide de cette méthode, sélectionnez la catégorie Utilisateurs, puis la tâche de gestion d'un utilisateur. Recherchez et sélectionnez l'utilisateur que vous souhaitez gérer. Dans les résultats de recherche, cliquez sur une icône pour afficher la liste des tâches que vous pouvez utiliser pour gérer l'utilisateur sélectionné. Dans cette liste, vous pouvez sélectionner la tâche Modifier l'utilisateur ou une autre tâche appropriée.

  Vous pouvez également configurer des listes de tâches dans des tâches autres que les tâches de gestion. Par exemple, vous pouvez ajouter une liste de tâches à un onglet Appartenance. Dans ce cas, une liste de tâches est disponible pour chaque membre figurant dans l'onglet Appartenance.

  Remarque : Seules les tâches que l'administrateur actuel peut utiliser s'affichent dans la liste de tâches d'un objet.

Tâches d'administration par défaut

CA IdentityMinder inclut des tâches et des rôles d'administration par défaut. Pour ajouter ces derniers à CA IdentityMinder, importez un fichier de définition de rôle dans la console de gestion. Lorsque vous créez un environnement dans la console de gestion et que vous choisissez de créer des rôles par défaut, CA IdentityMinder importe automatiquement un fichier de définition de rôle.

Remarque : Pour prendre en charge certaines fonctionnalités, telles que la gestion des comptes pour certains types de terminaux, vous pouvez importer d'autres fichiers de définition de rôle pour créer les rôles et les tâches dont vous avez besoin.

Dans la plupart des cas, vous pouvez utiliser les tâches installées par défaut. Toutefois, vous pouvez modifier l'onglet Profil dans les tâches d'utilisateur par défaut, telles que Créer un utilisateur, Modifier l'utilisateur et Afficher l'utilisateur. L'onglet Profil inclut tous les champs définis pour l'objet Utilisateur dans le fichier de configuration d'annuaire. Vous pouvez limiter le nombre de champs apparaissant dans l'onglet ou modifier les propriétés d'affichage des champs.

Remarque : Il est recommandé de créer une copie d'une tâche par défaut, plutôt que de la modifier directement.

Création d'une tâche d'administration personnalisée

Une *tâche d'administration* est une fonctionnalité administrative qu'un utilisateur peut exécuter dans Identity Manager. Par exemple, Créer un utilisateur, Modifier le groupe et Afficher l'appartenance à un rôle sont des tâches d'administration.

CA IdentityMinder inclut des tâches d'administration par défaut que vous pouvez modifier en fonction des besoins de votre entreprise.

Pour créer une tâche d'administration personnalisée, procédez comme suit :

Remarque : La section Conditions préalables pour Active Directory (page 72) inclut des informations supplémentaires si Identity Manager gère un magasin d'utilisateurs Active Directory.

1. Dans la console d'utilisateur Identity Manager, sélectionnez Rôles et tâches, Tâches d'administration, Créer une tâche d'administration.

   Identity Manager vous demande si vous souhaitez créer une nouvelle tâche ou créer une tâche basée sur une tâche existante.

   Par exemple, sélectionnez la tâche de modification d'un utilisateur comme base de la nouvelle tâche.

2. Sélectionnez Create a Copy of an Existing Task (Créer une copie d'une tâche existante), puis recherchez la tâche à copier.

   Remarque : Plutôt que de modifier la tâche par défaut directement, il est recommandé de modifier sa copie.

3. Lorsque vous cliquez sur OK, une fenêtre comportant les cinq onglets suivants s'affiche.

Onglet	Objectif	Consulter cette rubrique
Profil	Définir le profil de la tâche en cours de création	Définition du profil de la tâche (page 48)
Rechercher	Limiter l'étendue des objets gérés par la tâche	Définition de la portée de la tâche (page 56)
Onglets	Choisir et concevoir les onglets de la tâche	Choix des onglets de la tâche (page 67)
Champs	Afficher les champs utilisés dans tous les onglets	Affichage des champs de la tâche (page 71)
Evénements	Sélectionner un processus de flux de travaux pour chaque événement si l'environnement Identity Manager et la tâche utilisent un flux de travaux	Affectation de processus de flux de travaux à des événements (page 71)

Onglet	Objectif	Consulter cette rubrique
Utilisation du rôle	Affiche les rôles qui incluent la tâche en cours de modification ou d'affichage.	Affichage de l'utilisation du rôle (page 71)

Définition du profil de la tâche

L'onglet Profil inclut des paramètres généraux de la tâche.

Définition du profil de la tâche

1. Choisissez le type d'objet de la tâche, appelé objet principal, et l'action à effectuer sur ce type d'objet.
2. Remplissez les champs requis et cochez les cases nécessaires à la tâche.

   Remarque : Si vous créez une tâche comportant des paramètres de profil similaires à ceux d'une tâche existante, cliquez sur Copier le profil à partir d'une autre tâche. Cette option spécifie, pour la tâche que vous créez, les paramètres de profil d'une tâche existante que vous sélectionnez. Ajoutez ensuite un nom et une description pour la nouvelle tâche.
3. (Facultatif) Associez un gestionnaire de tâches métier à la tâche.
4. Une fois cet onglet renseigné, passez à l'étape suivante, Définition de la portée de la tâche (page 56).

Onglet Profil de tâche d'administration

L'onglet Profil de tâche d'administration permet de définir des paramètres généraux pour une tâche d'administration.

Cet onglet contient les champs suivant.

- **Nom**

  Définit le nom de la tâche.
- **Balise**

  Définit un identificateur unique pour la tâche. Elle est utilisée dans les URL, les services Web ou les fichiers de propriétés. La balise peut contenir des caractères ASCII (a-z, A-Z), des chiffres (0-9) ou des traits de soulignement, et commence par une lettre ou un trait de soulignement.
- **Description**

  Spécifie une remarque facultative sur l'objectif de la tâche.

- **Ordre des tâches**

  Spécifie l'ordre d'affichage de la tâche. Si aucun ordre n'est spécifié, les tâches sont affichées dans l'ordre alphabétique.

- **Catégorie**

  Spécifie une catégorie pour la tâche. Les catégories sont affichées sous forme d'onglets en haut de la fenêtre.

- **Ordre des catégories**

  Spécifie l'ordre dans lequel l'onglet de catégorie apparaît. Par exemple, si vous définissez l'ordre de catégorie sur 3, la catégorie que vous avez spécifiée apparaît en tant que troisième onglet.

- **Catégorie 2**

  Spécifie la catégorie de second niveau, qui apparaît sous la forme d'un lien au-dessous de la liste des onglets de catégories. La catégorie de second niveau apparaît que si l'onglet de la catégorie de premier niveau est sélectionné. Par exemple, si vous avez créé une tâche comportant la catégorie de premier niveau Employé et une catégorie de second niveau Gestion des employés, la catégorie Gestion des employés n'apparaît qu'une fois que vous avez sélectionné l'onglet Employé.

- **Catégorie 2 - Ordre**

  Spécifie l'ordre dans lequel la catégorie de second niveau apparaît, s'il existe plusieurs catégories de second niveau dans une catégorie principale.

- **Catégorie 3**

  Spécifie la catégorie de troisième niveau, qui apparaît dans le volet de navigation gauche. Les tâches sont répertoriées sous la catégorie de troisième niveau. Par exemple, dans un environnement par défaut, un utilisateur disposant du rôle Gestionnaire de systèmes ou Gestionnaire d'utilisateurs voit la catégorie de troisième niveau Gérer les utilisateurs lorsqu'il sélectionne l'onglet Utilisateurs.

- **Catégorie 3 - Ordre**

  Spécifie l'ordre dans lequel la catégorie de troisième niveau apparaît.

- **Objet principal**

  Spécifie l'objet sur lequel la tâche agit.

- **Action**

  Spécifie l'opération à effectuer sur l'objet.

- **Synchronisation des utilisateurs**

  Spécifie si la tâche synchronise ou non les utilisateurs avec les stratégies d'identité. Vous pouvez sélectionner l'une des options suivantes.

  - **Désactivé** (valeur par défaut)

    Indique que cette tâche ne déclenche pas la synchronisation des utilisateurs.

  - **A la fin de la tâche**

    Indique que CA IdentityMinder démarre le processus de synchronisation des utilisateurs une fois que tous les événements d'une tâche sont terminés. Ce paramètre est l'option de synchronisation par défaut des tâches Créer un utilisateur, Modifier un utilisateur et Supprimer un utilisateur. Le paramètre par défaut de toutes les autres tâches est Désactivé.

    Remarque : Si vous activez l'option A la fin de la tâche pour une tâche incluant plusieurs événements, CA IdentityMinder synchronise les utilisateurs uniquement lorsque tous les événements de la tâche sont terminés. Si l'un de ces événements ou plusieurs requièrent une approbation de flux de travaux, cela peut prendre plusieurs jours. Pour que CA IdentityMinder applique les stratégies d'identité avant la fin de tous les événements, activez l'option A chaque événement.

  - **A chaque événement**

    Indique que CA IdentityMinder démarre le processus de synchronisation des utilisateurs (page 291) à la fin de chaque événement d'une tâche.

    Pour les tâches comportant des événements principal et secondaire pour le même utilisateur, si vous définissez la synchronisation des utilisateurs sur l'option A chaque événement, il se peut que le nombre de stratégies d'identité appliquées à un utilisateur soit plus important que si vous aviez sélectionné l'option A la fin de la tâche.

- **Synchronisation des comptes**

  Synchronise les comptes existant sur le serveur de provisionnement, si le provisionnement est activé.

  - **Désactivé** (valeur par défaut)

    Indique que cette tâche ne déclenche pas la synchronisation des comptes.

  - **A la fin de la tâche**

    Indique que CA IdentityMinder démarre le processus de synchronisation des comptes une fois que tous les événements d'une tâche sont terminés.

- **A chaque événement**

  Indique que CA IdentityMinder démarre le processus de synchronisation des comptes à la fin de chaque événement d'une tâche.

  Remarque : Pour obtenir des performances optimales, sélectionnez A la fin de la tâche. Cependant, si vous sélectionnez l'option A la fin de la tâche pour une tâche incluant plusieurs événements, CA IdentityMinder synchronise les comptes uniquement lorsque tous les événements de la tâche sont terminés. Si l'un de ces événements ou plusieurs requièrent une approbation de flux de travaux, cela peut prendre plusieurs jours. Pour que CA IdentityMinder synchronise les comptes avant la fin de tous les événements, sélectionnez l'option A chaque événement.

- **Masquer dans les menus**

  Empêche la tâche d'apparaître dans les menus. Activez ce contrôle si la tâche n'est invoquée que par une URL ou par une autre tâche.

- **Tâche publique**

  Met la tâche à la disposition des utilisateurs qui ne se sont pas connectés à CA IdentityMinder. Les tâches publiques par défaut sont les tâches de mot de passe oublié et d'auto-enregistrement.

- **Activer l'audit**

  Enregistre des informations sur la tâche dans une base de données d'audit. Les informations d'audit permettent de générer des rapports. Reportez-vous au *manuel de configuration*.

- **Activer le flux de travaux**

  Permet aux événements CA IdentityMinder associés à la tâche de déclencher des processus de flux de travaux, si le moteur du flux de travaux est installé. Par exemple, les événements associés à la tâche Supprimer un groupe peuvent déclencher un processus de flux de travaux incluant une étape d'approbation.

- **Activer les services Web**

  Marque la tâche comme étant une tâche pour laquelle une sortie WSDL (Web Services Description Language) peut être générée via la console de gestion. Activez ce contrôle si vous souhaitez utiliser la soumission de tâches à distance. Pour plus d'informations, reportez-vous au *manuel Programming Guide for Java.*

- **Processus de flux de travaux**

  Autorise la configuration d'un flux de travaux de niveau tâche. Cliquez sur l'icône crayon pour configurer un flux de travaux qui utilise ou non une stratégie.

- **Priorité des tâches**

  Détermine l'ordre dans lequel CA IdentityMinder exécute les tâches. Les tâches présentant une priorité Elevée sont exécutées avant celles présentant une priorité Moyenne ou Faible. La priorité par défaut d'une tâche est Moyenne.

  Remarque : Vous pouvez utiliser la tâche Afficher les tâches soumises pour rechercher des tâches présentant une priorité spécifique, puis en afficher l'état.

- **Gestionnaires de tâches métier (GTM)**

  Associez un gestionnaire de tâches métier (page 76) à la tâche.

- **Boutons d'action du flux de travaux**

  Ajoutent des boutons d'action personnalisés aux tâches d'approbation de flux de travaux.

- **Copier le profil à partir d'une autre tâche**

  Copie des données à partir de l'onglet Profil d'une autre tâche.

  Par exemple, vous pouvez copier les paramètres de l'onglet Profil de la tâche Modifier un utilisateur, puis ajouter un nom et une description.

Propriétés de configuration de la tâche

Les propriétés de configuration de la tâche contrôlent les propriétés d'affichage et certains comportements.

Chemin d'accès à l'icône de la tâche

Spécifie l'URL d'une image utilisée comme icône pour cette tâche dans des listes de tâches.

Aperçu de l'icône de tâche

Affiche l'icône de la tâche telle qu'elle se présente dans des listes de tâches.

Supprimer la fonction de navigation dans les tâches

Lorsque cette option est sélectionnée, la navigation de niveau supérieure et la liste des tâches sont masquées lorsqu'un utilisateur sélectionne une tâche. Cela empêche les utilisateurs de quitter la tâche actuelle tant qu'ils n'ont pas terminé les actions requises ou annulé la tâche.

Fenêtre cible

Lorsque vous indiquez une valeur dans ce champ, CA IdentityMinder ouvre cette tâche dans une nouvelle fenêtre de navigation. Ce champ permet d'ouvrir une nouvelle fenêtre de navigation pour une tâche externe qui redirige les utilisateurs vers un autre site Web.

Vous pouvez spécifier un nom pour la fenêtre.

Remarque : N'utilisez pas ce champ pour ouvrir des tâches d'administration CA IdentityMinder dans une autre fenêtre de navigation. CA IdentityMinder ne prend pas en charge l'affichage de plusieurs fenêtres de navigation dans une même session utilisateur CA IdentityMinder.

Attributs personnalisés définis par l'utilisateur pour les rôles

CA IdentityMinder prend en charge les attributs personnalisés définis par l'utilisateur qui vous permettent de spécifier des informations complémentaires sur les rôles qui vous aident à filtrer les rôles de votre organisation. Par exemple, un environnement d'entreprise peut disposer de plus de mille rôles. Cette organisation peut spécifier des informations complémentaires, telles que l'unité commerciale ou la situation géographique, pour chaque rôle. L'administrateur peut alors utiliser ces informations pour faciliter les recherches de rôles.

Vous pouvez utiliser les attributs personnalisés dans les tâches Créer, Modifier et Afficher pour les rôles suivants.

- Rôles d'administration
- Rôles de provisionnement
- Rôle d'accès

Pour configurer des attributs personnalisés pour des rôles, procédez comme suit :

1. Ajoutez la prise en charge des attributs personnalisés à l'onglet Profil pour les tâches qui créent, modifient ou affichent des rôles d'administration, de provisionnement ou d'accès.
2. Configurez les fenêtres de recherche et de liste pour les rôles à inclure dans les attributs personnalisés.

Informations complémentaires :

Configuration des attributs personnalisés de l'onglet Profil pour les rôles (page 54)
Ajout d'attributs personnalisés aux définitions de fenêtres de recherche (page 55)

Configuration des attributs personnalisés de l'onglet Profil pour les rôles

CA IdentityMinder permet de configurer un maximum de 10 attributs personnalisés dans l'onglet Profil des tâches qui permettent de créer, de modifier ou d'afficher des rôles.

Pour configurer des attributs personnalisés dans l'onglet Profil :

1. Cliquez sur Rôles et Tâches, Tâches d'administration, Modifier les tâches d'administration.

   La page Sélectionner une tâche d'administration s'affiche.

2. Recherchez et sélectionnez la tâche d'administration que vous souhaitez modifier.

   CA IdentityMinder affiche les détails de la tâche d'administration sélectionnée.

3. Cliquez sur l'onglet Onglets.

   Les onglets configurés pour être utilisés avec cette tâche d'administration apparaissent.

4. Cliquez sur l'icône représentant une flèche pour modifier l'onglet Profil.

   La fenêtre Configurer le profil apparaît.

5. Activez la case à cocher en regard de chaque champ personnalisé à ajouter à l'onglet Profil, puis entrez une étiquette significative.
6. Cliquez sur OK.

   Les attributs personnalisés sont disponibles dans l'onglet Profil de la tâche modifiée une fois la tâche soumise.

   Remarque : Pour utiliser les attributs personnalisés dans les recherches de rôles, configurez la fenêtre de recherche (page 55) pour qu'elle affiche ces attributs personnalisés.

Ajout d'attributs personnalisés aux définitions de fenêtres de recherche

Pour filtrer des rôles dans CA IdentityMinder, vous pouvez seulement utiliser les attributs disponibles dans la fenêtre de recherche. Pour filtrer les rôles en fonction des attributs personnalisés définis, vous devez ajouter ces derniers à la fenêtre de recherche des rôles.

Pour ajouter des attributs personnalisés à la fenêtre de recherche des rôles :

1. Cliquez sur Rôles et Tâches, Tâches d'administration, Modifier les tâches d'administration.

   La page Sélectionner une tâche d'administration s'affiche.

2. Recherchez et sélectionnez la tâche d'administration que vous souhaitez modifier.

   Pour ajouter des attributs personnalisés aux fenêtres de recherche, sélectionnez la tâche Modifier ou Afficher pour le type de rôle (administration, provisionnement ou accès) incluant les attributs personnalisés.

   CA IdentityMinder affiche les détails de la tâche d'administration sélectionnée.

3. Cliquez sur l'onglet Rechercher dans la fenêtre Modifier le rôle d'administration.

   La fenêtre de détails de la recherche apparaît.

4. Cliquez sur Parcourir pour afficher la liste des définitions de fenêtres de recherche disponibles pour la tâche.

   La page Sélectionner une définition de fenêtre s'ouvre.

5. Sélectionnez une définition de fenêtre de recherche à modifier ou créez une copie d'une définition existante.

   La fenêtre Configure Standard search (Configurer la recherche standard) s'ouvre.

6. Ajoutez les attributs personnalisés aux tableaux suivants.

   ■ Sélectionner les champs de recherche

   ■ Sélectionner les champs des résultats de la recherche

7. Modifiez le nom de l'attribut personnalisé afin qu'il corresponde au nom que vous avez spécifié lorsque vous avez configuré l'onglet Profil.

8. Cliquez sur OK pour enregistrer les modifications apportées à la définition de fenêtre de recherche.

   La page Sélectionner une définition de fenêtre s'ouvre.

9. Sélectionnez la fenêtre que vous avez créée ou modifiée, puis cliquez sur Sélectionner.

10. Sélectionnez Tous les rôles d'administration dans la liste Options de recherche.
11. Cliquez sur Soumettre.

    La fenêtre de recherche inclut désormais les attributs personnalisés dans les options de recherche et affiche les attributs dans les résultats de la recherche.

Définition de la portée de la tâche

Dans l'onglet Rechercher, vous définissez la portée de la tâche, qui limite les objets accessibles à la tâche. Par exemple, si l'objet de la tâche est Utilisateurs, vous pouvez définir la portée sur les utilisateurs qui sont des sous-traitants.

Remarque : Si la tâche ne comporte pas d'objet principal ou si l'action est Auto-modification, Auto-affichage ou Approuver, l'onglet Rechercher n'apparaît pas.

Configurez les paramètres suivants dans l'onglet Rechercher :

Fenêtre de recherche

La fenêtre de recherche limite la portée de la tâche en fonction de filtres. Cliquez sur Parcourir pour afficher les options de fenêtre de recherche disponibles.

Remarque : Vous pouvez créer votre propre fenêtre de recherche (page 57). Pour créer une version modifiée d'une fenêtre de recherche existante, sélectionnez la fenêtre de recherche, puis cliquez sur OK. Vous pouvez alors modifier la fenêtre de recherche sans changer la définition de fenêtre de recherche d'origine. Pour créer une fenêtre de recherche, cliquez sur Nouveau.

Options de recherche

Les options de recherche n'apparaissent que si l'objet est un rôle ou un groupe.

- La première option limite la recherche en fonction des champs qui sont définis dans la fenêtre de recherche. En fonction de ces limites, la recherche localise tous les groupes ou rôles accessibles à l'administrateur.
- D'autres options limitent la recherche tel qu'indiqué.

Remarque :

- Par défaut, les fenêtres de recherche de groupes prennent en charge le filtrage. Cela signifie que l'administrateur peut spécifier des critères pour limiter la portée des recherches de groupes. Pour supprimer la fonctionnalité de filtrage, créez une fenêtre de recherche ne contenant aucun champ à inclure dans une requête de recherche.
- L'indication *Filtrage non pris en charge*, qui apparaît dans l'onglet Rechercher lorsque l'objet est un rôle, signifie que la tâche affiche les rôles qui correspondent aux critères de l'option que vous sélectionnez. Les champs de recherche configurés dans la fenêtre de recherche sont ignorés.

Les objets modifiés doivent rester dans la portée de l'administrateur.

Lorsque cette case à cocher est activée, CA IdentityMinder affiche une erreur si les modifications apportées à la tâche font que l'objet principal ne figure plus dans la portée de l'administrateur. Par exemple, un administrateur peut utiliser Modifier un utilisateur pour remplacer l'attribut Type d'employé d'un utilisateur par Gestionnaire. Cette modification peut placer l'utilisateur en dehors de la portée de l'administrateur.

Configuration d'une fenêtre de recherche

Vous configurez une fenêtre de recherche pour limiter la portée de la tâche et contrôler les champs sur lesquels l'utilisateur peut effectuer une recherche. Les fenêtres de recherche s'appliquent à deux types d'objets :

- Un *objet principal* : l'objet que la tâche doit modifier ou afficher.
- Un *objet secondaire* : l'objet associé à l'objet principal.

  Par exemple, si vous incluez un onglet de groupe dans une tâche Créer un utilisateur, l'utilisateur est l'objet principal et le groupe l'objet secondaire. L'onglet de groupe nécessite une fenêtre de recherche pour les groupes.

  Remarque : Après avoir configuré une fenêtre de recherche, vous pouvez l'utiliser pour n'importe quelle tâche afin de rechercher un objet principal ou secondaire.

Filtres de recherche

Les filtres de recherche limitent les objets retournés par la recherche. Par exemple, si l'objet est Utilisateurs, vous pouvez limiter la recherche pour qu'elle ne trouve que des sous-traitants. Vous pouvez configurer un filtre pour rechercher les utilisateurs dont le type d'employé est Sous-traitant.

Vous pouvez configurer des recherches sur les champs ci-après.

Afficher uniquement les objets correspondant aux règles suivantes

Définit des critères supplémentaires à combiner avec le filtre défini par l'utilisateur pour affiner la recherche.

Prenez note des points suivants lors de l'utilisation de ce champ**.**

- En raison des limites dont les recherches de rôles de provisionnement font l'objet, ces critères écrasent les champs de filtre portant le même nom entré par l'utilisateur.
- Les attributs utilisés lorsque vous configurez ce champ ne doivent pas être ajoutés comme des champs de recherche disponibles dans la fenêtre de recherche.

  Par exemple, si vous configurez l'écran de recherche pour n'afficher que les rôles lorsque l'attribut activé est Oui, supprimez l'attribut activé de la liste des attributs que les utilisateurs peuvent spécifier comme critère de recherche.

  Sinon, le critère entré par l'utilisateur est ignoré.

Filtre de recherche par défaut

Définit un filtre qui s'affiche par défaut lorsqu'un administrateur utilise la fenêtre de recherche. Par exemple, si vous configurez une fenêtre de recherche pour la tâche Modifier un sous-traitant et savez que les administrateurs recherchent généralement les sous-traitants en fonction du nom de la société du contrat, vous pouvez définir le filtre par défaut sur Société du contrat = *. Les administrateurs peuvent remplacer le filtre par défaut en spécifiant des critères de recherche différents. Définir un filtre par défaut améliore les performances en limitant le nombre de résultats retournés si un administrateur ne spécifie pas de filtre avant de commencer une recherche.

Sélectionner automatiquement tous les résultats de recherche utilisés avec les tâches de multisélection

Indique que tous les résultats de recherche sont sélectionnés par défaut. Si vous activez cette case à cocher, tous les objets figurant dans la liste des résultats de recherche apparaissent accompagnés d'une case cochée.

Recherche automatique

Indique qu'un champ de recherche est affiché avec les résultats de recherche.

Définir automatiquement le sujet de la tâche pour les résultats de recherche unique

Définit automatiquement l'objet principal de la tâche lorsqu'un seul objet correspond au filtre de recherche.

Par exemple, supposons que cette option soit sélectionnée pour une fenêtre de recherche d'utilisateurs associée à la tâche Modifier l'utilisateur. Lorsqu'un administrateur ouvre la tâche Modifier l'utilisateur et entre un filtre de recherche qui ne retourne qu'un seul utilisateur, CA IdentityMinder ouvre la tâche Modifier l'utilisateur pour cet utilisateur. L'administrateur n'a pas besoin de sélectionner l'utilisateur pour ouvrir cette tâche.

Remarque : Pour appliquer ce paramètre, la recherche automatique doit également être sélectionnée.

Enregistrer le filtre de recherche

Indique que le filtre de recherche de la tâche est enregistré pour l'utilisateur de la session actuelle. La prochaine fois qu'un utilisateur effectue une recherche dans la tâche, le filtre de recherche enregistré est affiché.

Remarque : CA IdentityMinder enregistre le filtre de recherche pour la durée de la session de l'utilisateur. Le filtre de recherche est effacé lorsque l'utilisateur se déconnecte.

Rechercher dans l'organisation

Affiche un filtre d'organisation dans la fenêtre de recherche. Si cette case à cocher est activée, l'administrateur peut spécifier un filtre qui limite les organisations dans lesquelles CA IdentityMinder recherche un objet. Vous pouvez spécifier des valeurs par défaut pour le filtre de recherche d'organisations en spécifiant une fenêtre de recherche dans le champ Recherche d'organisation.

Enregistrer l'organisation de recherche

Indique que l'organisation de la tâche est enregistrée si une organisation a été établie pour la recherche. La prochaine fois qu'un utilisateur effectue une recherche dans la tâche, l'organisation est affichée.

Recherche d'organisation

Spécifie la fenêtre de recherche que CA IdentityMinder utilise pour permettre aux administrateurs de rechercher une organisation.

Portée de la recherche d'une organisation par défaut

Spécifie la portée de la recherche d'une organisation par défaut qui apparaît lorsqu'un administrateur utilise une fenêtre de recherche. La portée de la recherche détermine les niveaux d'une arborescence organisationnelle qui sont inclus dans la recherche. L'administrateur peut remplacer la portée de la recherche d'une organisation par défaut en spécifiant des critères de recherche différents dans la fenêtre de recherche.

Par exemple, si vous configurez une fenêtre de recherche pour une tâche Modifier un sous-traitant personnalisée dans un environnement qui enregistre les informations en relation avec les sous-traitants à divers niveaux de l'arborescence organisationnelle, vous pouvez définir la portée de la recherche d'une organisation par défaut sur Et moins que.

Rechercher une expression unique

Définit le type de filtre de recherche qui s'affiche dans la fenêtre de recherche. Si cette case est cochée, l'utilisateur peut spécifier un filtre de recherche unique, tel que <attribut><comparateur><valeur>. Si elle n'est pas cochée, l'utilisateur peut spécifier plusieurs filtres de recherche. Par exemple, <attribut1><comparateur><valeur1> AND <attribut2><comparateur> <valeur2>. Les objets remplissant les conditions définies par tous les filtres sont retournés dans les résultats de recherche. Dans l'exemple précédent, les objets incluant <valeur1> et <valeur2> sont retournés comme résultats de recherche.

Recherche en mode Est égal(e) à

Interdit aux administrateurs d'utiliser des opérateurs de recherche autres que l'opérateur Est égal(e) à.

Afficher le nombre de résultats

Affiche le nombre de résultats de recherche correspondant. Lorsque cette case à cocher est activée, toutes les recherches retournent le message "Il y a X résultats".

Ajouter un bouton de tâche pour <nom_de_la_tâche>

Ajoute un lien vers une autre tâche dans la fenêtre de recherche. Le lien est affiché sous forme de bouton.
Ce champ est généralement utilisé pour ajouter une tâche de création à une fenêtre de recherche configurée pour la navigation objet/tâche.

Etiquette facultative

Spécifie une étiquette pour la tâche sélectionnée dans le champ précédent. Cette étiquette s'affiche sur le bouton de la tâche.

Ajouter un bouton de suppression multiple pour <nom_de_la_tâche>

Ajoute à une tâche un lien qui permet à l'administrateur de sélectionner plusieurs objets à supprimer. Le lien est affiché sous forme de bouton.
Ce champ est généralement utilisé avec la navigation objet/tâche.

Champs et résultats de recherche

Dans une autre partie de la fenêtre de recherche, vous sélectionnez les champs que l'administrateur peut utiliser dans une requête de recherche, ainsi que les champs à afficher dans les résultats de recherche.

Sélectionner les champs de recherche

Sélectionnez les champs que l'administrateur peut utiliser pour créer une requête de recherche.

Pour ajouter des champs supplémentaires, sélectionnez des champs dans la zone de liste en dessous du tableau des champs de recherche.

Une fois les champs sélectionnés, vous pouvez changer l'ordre dans lequel ils apparaissent à l'aide des icônes représentant une flèche vers le haut et vers le bas situées à droite du champ.

Remarque : Si vous ne spécifiez pas les champs que l'administrateur peut utiliser, CA IdentityMinder démarre la recherche automatiquement.

Sélectionner les champs des résultats de la recherche

Sélectionnez les champs qu'CA IdentityMinder affiche dans les résultats de recherche. Vous pouvez sélectionner des champs non disponibles dans la requête de recherche.

Pour ajouter des champs supplémentaires, sélectionnez des champs dans la zone de liste en dessous du tableau des champs de recherche.

Style

Lorsque vous sélectionnez un champ à afficher dans les résultats de recherche, vous pouvez sélectionner l'une des options de style suivantes :

- **Nom d'affichage booléen**

  Affiche le nom du champ pour tous les résultats qui sont vrais (True). Par exemple, si vous entrez Activé comme nom de l'attribut qui indique l'état de compte d'un utilisateur, Activé s'affiche dans les résultats de recherche pour tous les comptes d'utilisateurs actifs.

- **Coche**

  Affiche la valeur sous la forme d'une coche sélectionnée en fonction de la valeur de l'attribut. Par exemple, si vous sélectionnez le style Coche pour représenter l'état Activé/Désactivé de comptes d'utilisateurs, CA IdentityMinder affiche une coche sélectionnée pour tous les comptes actifs.

- **Chaîne à valeurs multiples**

  Affiche les valeurs d'un attribut à valeurs multiples sur des lignes séparées. Les valeurs sont répertoriées dans l'ordre alphabétique.

- **Case à cocher en lecture seule**

  Affiche la valeur sous forme de case à cocher en lecture seule.

- **Chaîne**

  Affiche la valeur sous forme de chaîne de texte.

- **Tâche**

  Ajoute une liste de tâches à un champ. L'utilisateur clique sur une icône représentant une flèche pour afficher la liste des tâches qu'il peut effectuer sur l'objet associé au champ de recherche. Par exemple, si vous ajoutez une liste de tâches à un champ Nom dans les résultats de recherche, l'utilisateur peut cliquer sur l'icône flèche figurant dans ce champ pour afficher la liste des tâches qu'il peut effectuer sur l'utilisateur qu'il sélectionne.

  Ce paramètre peut également être utilisé pour faire apparaître une valeur d'attribut comme un lien vers une tâche.

  Si vous sélectionnez le style Tâche, une icône représentant une flèche vers la droite apparaît en regard de la colonne Style. Cliquez sur la flèche pour ouvrir la boîte de dialogue Propriétés du champ. Utilisez cette boîte de dialogue pour configurer une liste de tâches.

- **Liste des tâches**

  Permet d'ajouter des tâches supplémentaires que les utilisateurs peuvent effectuer au niveau des objets dans les fenêtres de recherche et de liste. Par exemple, vous pouvez configurer la fenêtre de recherche dans la tâche Modifier un utilisateur de façon à permettre aux utilisateurs d'effectuer une tâche, comme désactiver un utilisateur de la liste d'utilisateurs renvoyés par la recherche.

  Lorsque vous sélectionnez cette option, vous déterminez si les utilisateurs accèdent à la tâche en cliquant sur une icône ou sur un lien de texte.

- **Menu des tâches**

  Permet d'ajouter des tâches supplémentaires (similaires au style Liste des tâches) en tant qu'éléments de menu contextuel.

  Lorsque vous sélectionnez cette option, un bouton Action s'affiche à côté de chaque objet dans une fenêtre de recherche ou de liste. Les utilisateurs doivent cliquer sur le bouton Action pour voir la liste des tâches qu'ils sont autorisés à effectuer au niveau de cet objet.

Remarque : Pour voir les options des styles Liste des tâches et Menu des tâches, sélectionnez Séparateur lorsque vous ajoutez un champ à la table des résultats de la recherche. Pour plus d'informations sur l'ajout de tâches supplémentaires aux fenêtres de recherche et de liste, consultez le manuel *User Console Design Guide*.

Triable

Cochez cette case pour permettre à l'administrateur de trier les résultats de recherche en fonction d'un ou plusieurs champs.

Définir l'ordre de tri par défaut des résultats de la recherche

Détermine l'ordre dans lequel les résultats de recherche sont affichés. Les résultats de recherche sont d'abord triés en fonction du premier champ figurant dans la liste, puis en fonction de chacun des champs supplémentaires dans l'ordre dans lequel ils apparaissent. Cochez la case Décroissant pour trier les résultats dans l'ordre décroissant.

Sélectionner des objets contenant des champs *nom de champ* modifiés

Spécifie que les objets dans lesquels le champ spécifié a été modifié sont sélectionnés lorsque l'utilisateur clique sur le bouton Sélectionner.

Retourner *N* résultats par page

Sélectionnez le nombre de résultats à afficher par page. Si les résultats de recherche dépassent le nombre spécifié, CA IdentityMinder affiche un lien vers chaque page de résultats.

Aide sur les fenêtres de recherche définie par l'utilisateur

Si vous souhaitez ajouter du texte personnalisé à votre fenêtre de recherche, vous pouvez définir votre texte dans la zone de texte HTML correspondante. Vous pouvez ajouter du texte dans les zones suivantes :

- Début ou fin de la page
- Avant ou après la création
- Avant ou après les résultats

Types de fenêtres de recherche

Identity Manager inclut les fenêtres de recherche préconfigurées suivantes.

Fenêtre de recherche de rôles d'accès

La fenêtre de recherche de rôles d'accès permet de configurer des filtres de recherche pour trouver des rôles d'accès correspondant à des critères spécifiques.

Fenêtre de recherche de tâche d'accès

La fenêtre de recherche de tâche d'accès permet de configurer des filtres de recherche pour trouver des tâches d'accès correspondant à des critères spécifiques. Cette fenêtre de recherche est utilisée pour trouver une tâche d'accès à afficher ou à modifier ou pour ajouter une tâche à un rôle d'accès.

Fenêtre de recherche de rôles d'administration

La fenêtre de recherche de rôles d'administration permet de configurer des filtres de recherche pour trouver des rôles d'administration correspondant à des critères spécifiques.

Fenêtre de recherche de tâches d'administration

La fenêtre de recherche de tâches d'administration permet de configurer des filtres de recherche pour trouver des tâches d'administration correspondant à des critères spécifiques. Cette fenêtre de recherche est utilisée pour trouver une tâche d'administration à afficher ou à modifier ou pour ajouter une tâche à un rôle d'administration.

Fenêtre de recherche d'approbations

La fenêtre de recherche d'approbations permet de configurer l'affichage qui apparaît en haut d'une tâche d'approbation.

Fenêtre de recherche d'un utilisateur du processus de certification initiale

La fenêtre de recherche d'un utilisateur du processus de certification initiale permet de configurer des filtres de recherche afin de trouver des utilisateurs pour lesquels définir l'état sur certification requise. L'état de certification des utilisateurs sélectionnés est défini sur *certification requise*.

Fenêtre de recherche d'utilisateurs à certifier

La fenêtre de recherche d'utilisateurs à certifier permet de configurer des filtres de recherche pour trouver les utilisateurs nécessitant une certification.

Fenêtre de recherche de délégations

La fenêtre de recherche de délégations permet de configurer des filtres de recherche pour trouver d'autres utilisateurs à ajouter en tant que délégués. Un délégué est un autre utilisateur que vous pouvez temporairement autoriser à afficher et à résoudre vos tâches de flux de travaux.

Fenêtre de recherche d'utilisateurs à activer/désactiver

La fenêtre de recherche d'utilisateurs à activer/désactiver permet de configurer des filtres de recherche pour activer/désactiver des utilisateurs correspondant à des critères spécifiques.

Fenêtre de recherche d'un utilisateur du processus de certification finale

La fenêtre de recherche d'un utilisateur du processus de certification finale permet de configurer des filtres de recherche pour identifier les utilisateurs dont le cycle de certification doit être terminé.

Fenêtre de recherche d'un contrat de licence de l'utilisateur final

La fenêtre de recherche d'un contrat de licence de l'utilisateur final permet de configurer la tâche Auto-enregistrement avec une page spécifique à votre application d'identités.

Fenêtre de recherche d'exploration et de corrélation

La fenêtre de recherche d'exploration et de corrélation permet de configurer des filtres de recherche pour des définitions d'exploration et de corrélation correspondant à des critères spécifiques.

Fenêtre de recherche de fichier de chargeur à télécharger

La fenêtre de recherche de fichier de chargeur à télécharger permet de rechercher le fichier de chargeur à télécharger. Un fichier de chargeur permet d'automatiser les actions répétitives effectuées sur un grand nombre d'objets gérés.

Fenêtre de recherche du mot de passe oublié/de l'ID d'utilisateur oublié

La fenêtre de recherche du mot de passe oublié permet de configurer la tâche Mot de passe oublié pour inviter l'utilisateur à entrer les informations prouvant son identité.

Fenêtre de recherche de groupes

La fenêtre de recherche de groupes permet de configurer des filtres de recherche pour des groupes, tels que des groupes situés dans l'organisation financière.

Fenêtre de recherche d'un ensemble de stratégies d'identité

La fenêtre de recherche d'un ensemble de stratégies d'identité permet de configurer des filtres de recherche pour trouver des ensembles de stratégies d'identité correspondant à des critères spécifiques.

Fenêtre de recherche d'un gestionnaire d'attributs logiques

La fenêtre de recherche d'un gestionnaire d'attributs logiques permet de configurer des filtres de recherche pour trouver des gestionnaires d'attributs logiques. Cette fenêtre de recherche est utilisée pour trouver un gestionnaire d'attributs logiques afin d'en afficher ou d'en modifier la configuration.

Fenêtre de recherche de gestion des rapports

La fenêtre de recherche de gestion des rapports permet de configurer des filtres de recherche pour trouver un rapport à afficher ou à supprimer.

Fenêtre de recherche d'un utilisateur non certifié

La fenêtre de recherche d'un utilisateur non certifié permet de configurer des filtres de recherche pour trouver les utilisateurs non certifiés à la fin de la période de certification.

Fenêtre de recherche d'organisations

La fenêtre de recherche d'organisations permet de configurer des filtres de recherche pour limiter le choix d'organisations à certaines sous-organisations.

Fenêtre de recherche de rôles de provisionnement

La fenêtre de recherche de rôles de provisionnement permet de configurer des filtres de recherche pour extraire des rôles de provisionnement.

Fenêtre de recherche de modèles de comptes

La fenêtre de recherche de modèles de comptes vous permet de configurer des filtres de recherche pour extraire des modèles de comptes.

Fenêtre de recherche d'une stratégie de mot de passe

La fenêtre de recherche d'une stratégie de mot de passe permet de configurer des filtres de recherche pour trouver des stratégies de mot de passe correspondant à des critères spécifiques.

Fenêtre de recherche de définition de cliché

La fenêtre de recherche de définition de cliché permet de configurer des filtres de recherche pour trouver une définition de cliché à afficher, à modifier ou à supprimer.

Fenêtre standard de recherche

La fenêtre standard de recherche permet de configurer des filtres pour trouver des objets gérés personnalisés.

Fenêtre de recherche d'utilisateurs

La fenêtre de recherche d'utilisateurs permet de configurer des filtres de recherche pour trouver des utilisateurs correspondant à des critères spécifiques. Par exemple, vous pouvez rechercher des utilisateurs qui sont des sous-traitants.

Une fois l'onglet Rechercher renseigné, choisissez les onglets de la tâche.

Choix des onglets de la tâche

Dans l'onglet Onglets, nommez et configurez les onglets ; chaque onglet constitue un ensemble de champs que vous incluez dans la tâche. Vous pouvez inclure des onglets par défaut ou créer de nouveaux onglets. Par exemple, la tâche Modifier un utilisateur inclut les onglets suivants :

- Profil
- Rôle d'accès
- Rôles d'administration
- Groupes
- Déléguer des tâches

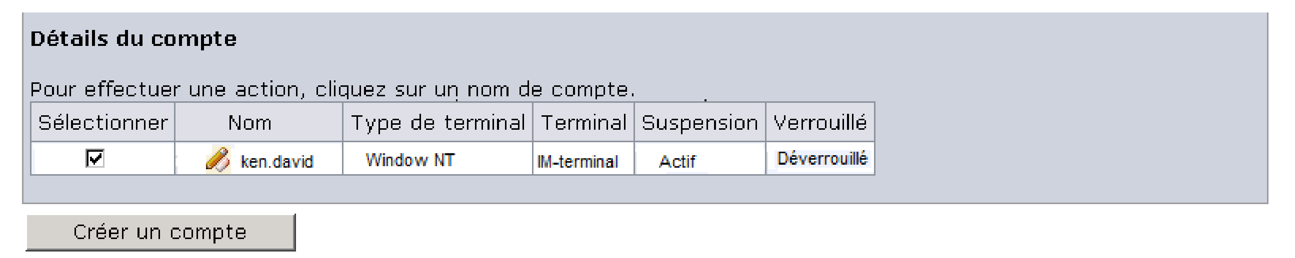
Pour modifier la définition d'un onglet, cliquez sur l'icône Modifier ( ) en regard du nom de l'onglet.

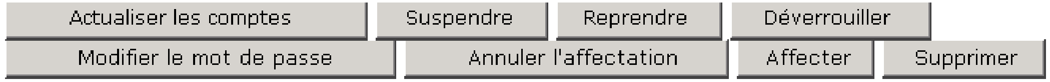
Informations complémentaires :

Onglet Comptes (page 68)
Onglet Planifier (page 70)

Onglet Comptes

L'onglet Comptes répertorie les comptes dans les terminaux gérés pour les utilisateurs disposant de rôles de provisionnement. En général, cet onglet est ajouté à des tâches permettant d'afficher ou de modifier un utilisateur.





Lorsque l'onglet Comptes est ajouté à une tâche Modifier un utilisateur, l'administrateur peut effectuer d'autres actions sur les comptes de l'utilisateur. comme les exemples ci-dessous.

- Suspendre ou reprendre un compte
- Déverrouiller un compte ayant été automatiquement verrouillé suite à un accès incorrect ou inapproprié. Par exemple, un compte peut être verrouillé lorsqu'un utilisateur dépasse le nombre acceptable d'échecs de tentatives de connexion défini dans une stratégie de mot de passe d'Identity Manager.
- Changer le mot de passe de l'utilisateur dans un ou plusieurs comptes
- Affecter des comptes à un utilisateur ou annuler l'affectation de ses comptes

Pour obtenir des détails sur les autres options définissables dans l'onglet Comptes, voir l'aide de la console d'utilisateur concernant l'onglet Configuration des comptes.

Conditions préalables à l'utilisation de l'onglet Comptes

Pour utiliser l'onglet Comptes, Identity Manager doit être configuré avec une prise en charge de provisionnement et son environnement doit inclure un annuaire de provisionnement.

Remarque : Pour configurer une prise en charge de provisionnement pour un environnement, reportez-vous au *Manuel de configuration*.

Champs de l'onglet Comptes

L'onglet Comptes affiche des détails sur les comptes que l'utilisateur possède au niveau des terminaux.

Voici certains des champs les plus significatifs :

- Nom : nom de connexion, nom de courriel ou autre nom du compte.
- Type de terminal : type de terminal (par exemple, un annuaire LDAP) associé au compte.
- Terminal : terminal spécifique associé au compte.
- Suspendu : un des trois états.
    - Actif s'affiche si le compte est activé.
    - Suspendu s'affiche si le compte est désactivé.
    - Activation manuelle en attente s'affiche s'il n'est pas possible de le reprendre ou de le suspendre. Connectez-vous au terminal pour reprendre ou suspendre le compte.
    - Non disponible s'affiche si l'état ne peut pas être récupéré en raison de l'absence de communication avec le terminal.
- Verrouillé : indique si le compte est verrouillé. Le verrouillage se produit lorsqu'un utilisateur tente à plusieurs reprises de se connecter au compte avec un mot de passe incorrect. Non disponible s'affiche si l'état ne peut pas être récupéré en raison de l'absence de communication avec le terminal.

Autres fonctionnalités de l'onglet Comptes

Lorsque l'onglet Comptes est inclus dans une tâche qui modifie un utilisateur, l'administrateur peut utiliser cette tâche pour exécuter des fonctionnalités sur les comptes de l'utilisateur. Les fonctionnalités disponibles dépendent de la configuration de l'onglet.

Vous pouvez choisir quelles fonctionnalités sont disponibles en utilisant l'option Modifier la tâche d'administration sur une tâche contenant l'onglet Comptes. Modifiez l'onglet Comptes pour déterminer si des fonctionnalités telles que Affecter un compte et Annuler l'affectation du compte sont disponibles sous l'onglet.

Pour plus d'informations, reportez-vous à l'aide en ligne de l'onglet Configurer des comptes.

Onglet Planifier

La planification permet d'automatiser l'exécution d'une tâche à une date ultérieure. Si vous planifiez une tâche associée à un flux de travaux, CA IdentityMinder exécute toutes les tâches tel que défini dans ce flux de travaux. Le statut des tâches planifiées peut être affiché dans la page Afficher les tâches soumises.

Une tâche planifiée que CA IdentityMinder n'a pas encore exécutée peut être annulée à l'aide de la page Afficher les tâches soumises.

Remarque : Si vous resoumettez une tâche planifiée qui a été annulée, celle-ci s'exécute immédiatement, quelle que soit l'heure d'exécution planifiée.

CA IdentityMinder fournit le planificateur en tant qu'onglet spécial. Pour accéder au planificateur, vous devez configurer une tâche avec l'onglet Planifier.

Ajout de l'onglet Planifier à une tâche d'administration

CA IdentityMinder permet de planifier des tâches à exécuter à une date et à une heure spécifiques. Pour planifier une tâche, vous devez ajouter l'onglet Planifier à une tâche d'administration.

Remarque : Vous ne pouvez pas ajouter l'onglet Planifier à toutes les tâches d'administration dans CA IdentityMinder. Si la tâche ne peut pas être planifiée, l'onglet Planifier n'est pas disponible dans la fenêtre Modifier la tâche d'administration.

Ajout de l'onglet Planifier à une tâche d'administration

1. Cliquez sur Rôles et tâches, Tâches d'administration, puis Modifier la tâche d'administration.

   La page Sélectionner une tâche d'administration s'affiche.

2. Sélectionnez Nom ou Catégorie dans le champ Où, puis entrez la chaîne que vous souhaitez rechercher et cliquez sur Rechercher.

   CA IdentityMinder affiche les tâches d'administration qui répondent à vos critères de recherche.

3. Choisissez une tâche d'administration, puis cliquez sur Sélectionner.

   CA IdentityMinder affiche les détails de la tâche d'administration sélectionnée.

4. Cliquez sur Onglets.

   Les onglets configurés pour la tâche d'administration sélectionnée s'affichent.

5. Sélectionnez Planifier dans la liste déroulante Quels onglets doivent apparaître dans cette tâche ? et cliquez sur .

   L'onglet Planifier est ajouté à la liste des onglets allant apparaître dans la tâche d'administration sélectionnée.

6. Cliquez sur Soumettre.

   L'onglet Planifier est ajouté à la tâche d'administration sélectionnée.

Affichage des champs de la tâche

Dans l'onglet Champs, vous pouvez afficher les champs qui s'appliquent à cette tâche. Ces champs sont les champs créés dans les onglets de cette tâche. Pour modifier les champs utilisés, retournez à l'onglet Onglets et sélectionnez l'onglet à modifier.

Une fois cet onglet renseigné, passez à l'étape suivante, Affectation de processus de flux de travaux à des événements (page 71).

Cependant, si cet environnement Identity Manager n'utilise pas de flux de travaux, vous pouvez maintenant cliquer sur Soumettre. Un message apparaît indiquant si la tâche a réussi. Si elle a réussi, vous pouvez l'ajouter à un rôle afin que les membres de rôles puissent commencer à l'utiliser.

Affichage de l'utilisation du rôle

L'onglet Utilisation du rôle permet d'afficher les rôles qui incluent la tâche que vous consultez ou modifiez.

Les propriétaires de rôles peuvent supprimer des tâches des rôles et en ajouter.

Remarque : Rôles d'administration par défaut inclut la liste des tâches des rôles d'administration installés par défaut avec CA IdentityMinder.

Affectation de processus de flux de travaux à des événements

Si vous avez activé le flux de travaux pour cet environnement Identity Manager, utilisez l'onglet Evénements afin de sélectionner un processus de flux de travaux pour chaque événement déclenché par la tâche. Le processus de flux de travaux que vous sélectionnez remplace celui sélectionné par défaut dans la console de gestion Identity Manager.

Pour plus d'informations sur les mappages de flux de travaux par défaut, reportez-vous au chapitre Paramètres avancés du *Manuel de configuration*.

Pour terminer de créer cette tâche, cliquez sur Soumettre. Un message apparaît indiquant si la tâche a réussi. Si elle a réussi, vous pouvez l'ajouter à un rôle afin que les membres de rôles puissent commencer à l'utiliser.

Prérequis Active Directory

Si Active Directory est le magasin d'utilisateurs, avant de créer des tâches d'administration, il peut être nécessaire de configurer certaines fonctionnalités Active Directory.

Attribut sAMAccountName

L'attribut sAMAccountName s'applique aux utilisateurs et aux groupes. Cet attribut est requis et dois être inclus dans les fenêtres de tâches utilisées pour créer les utilisateurs et les groupes.

Remarque : Lors de la création d'utilisateurs, la valeur de l'attribut sAMAccountName ne peut pas dépasser 20 caractères. Cette restriction ne s'applique pas aux groupes.

Vous pouvez écrire un gestionnaire d'attributs logiques personnalisé qui génère automatiquement un attribut sAMAccountName unique lorsqu'un utilisateur ou un groupe est créé. Dans ce cas, vous pouvez inclure l'attribut sAMAccountName en tant que champ masqué dans les fenêtres Créer un utilisateur et Créer un groupe.

Pour plus d'informations, reportez-vous au chapitre Attributs logiques du *Manuel de programmation Java*.

Type et portée de groupe

Il existe deux types de groupes dans Active Directory :

- Sécurité : ces groupes sont répertoriés dans les listes ACL (Access Control List), qui définissent les autorisations liées aux ressources et aux objets.
- Distribution : ces groupes sont utilisés pour regrouper des objets (par exemple, des utilisateurs et des groupes). Les groupes de distribution ne peuvent pas être utilisés pour accorder des autorisations dans Active Directory.

Chaque type de groupe a une portée qui détermine les éléments suivants :

- Emplacement des membres : endroit où peuvent résider les membres potentiels
- Autorisations : endroit où le groupe peut être utilisé pour les autorisations d'accès (si le groupe est un groupe de sécurité)
- Appartenance au groupe dans d'autres groupes : emplacement des groupes auxquels le groupe peut appartenir

Chaque type de groupe peut avoir l'une des portées suivantes :

Portée	**Emplacement des membres :**	**Autorisations**	**Appartenance au groupe dans d'autres groupes**
Universel	Les membres de groupes peuvent être des groupes Universel, des groupes Global, ainsi que des utilisateurs issus de n'importe quel domaine dans la forêt.	Peuvent être utilisés pour autoriser l'accès dans n'importe quel domaine d'une forêt.	Peuvent être des membres des groupes Domaine local et Universel dans n'importe quel domaine de la forêt.
Global	Les membres de groupes peuvent être des groupes Global et des utilisateurs situés dans le même domaine que le groupe.	Peuvent être utilisés pour autoriser l'accès dans n'importe quel domaine d'une forêt.	Peuvent être des membres des groupes Domaine local et Universel dans n'importe quel domaine de la forêt.
Domaine local	Les membres de groupes peuvent être des groupes Universel, des groupes Global, ainsi que des utilisateurs issus de n'importe quel domaine dans la forêt. Les membres peuvent également être des groupes Domaine local issus du même domaine.	Ne peuvent être utilisés que pour autoriser l'accès au domaine dans lequel le groupe réside.	Ne peuvent être que des membres d'autres groupes Domaine local dans le domaine.

Le type et la portée de groupe ne sont pas des attributs requis ; cependant, si vous ne spécifiez ni type ni portée de groupe, Active Directory crée un groupe de sécurité à portée globale.

Pour créer des groupes de type différent, vous pouvez créer un gestionnaire d'attributs logiques personnalisé. Reportez-vous au chapitre Attributs logiques du *Manuel de programmation Java*.

Une fois ces fonctionnalités Active Directory configurées, passez à l'étape suivante : Création d'une tâche d'administration.

Tâches externes pour fonctionnalités d'application

Une tâche externe effectue les opérations suivantes :

- Permet à un administrateur d'exécuter une fonction dans une application autre que CA IdentityMinder à partir de la console d'utilisateur.
- Le cas échéant, transmet des informations à l'application pour générer des tâches d'utilisateur, de groupe ou d'organisation.

Par exemple, une tâche externe peut transmettre des informations sur une organisation à une application générant des bons de commande. L'administrateur effectuant la tâche peut afficher les bons de commande ouverts de l'organisation via la console d'utilisateur.

Vous pouvez afficher des tâches externes en ouvrant l'application dans une nouvelle fenêtre de navigation ou en les affichant sous forme d'onglets dans une tâche d'administration CA IdentityMinder.

Deux onglets sont disponibles pour les tâches externes. Ces onglets sont configurés de la même manière mais fonctionnent différemment.

- L'onglet externe est un onglet visuel, ce qui signifie que la tâche affiche le contenu de l'URL dans un onglet.
- L'onglet d'URL externe est un onglet non visuel, ce qui signifie que la tâche redirige l'utilisateur vers l'URL entrée.

Onglet externe

Un onglet externe peut être ajouté à n'importe quelle tâche de création, d'affichage ou de modification pour en faire une tâche externe. Par exemple, si vous ajoutez un onglet externe à une tâche Créer un utilisateur, il apparaît dans cette tâche.

Pour un onglet externe :

- Aucun événement n'est généré pour une tâche externe.
- Si vous le souhaitez, vous pouvez utiliser des objets gérés.

- Dans le champ URL externe, vous pouvez spécifier l'adresse de l'application comme :
  - Adresse complète, incluant le nom de domaine complet ; par exemple :

    http://server1,mycompany.org/report/viewUserReport
  - Chemin relatif ; par exemple :

    /report/viewUserReport

    Si vous spécifiez le chemin relatif, Identity Manager ajoute automatiquement le nom de domaine complet du serveur sur lequel il est installé.
- Vous configurez les attributs à transmettre à l'application dans l'onglet Profil.

Onglet d'URL externe

Vous pouvez ajouter un onglet d'URL externe à une tâche d'affichage, telle qu'Afficher un utilisateur. Lorsque vous utilisez la tâche Afficher un utilisateur, vous êtes redirigé vers le site Web identifié par l'URL. Aucun autre onglet n'est visible.

Pour un onglet externe :

- L'onglet d'URL externe doit être le seul onglet de la tâche. Si d'autres onglets sont associés à la même tâche, l'onglet externe ne redirige pas l'utilisateur vers l'URL spécifiée.
- La tâche peut générer des événements pouvant faire l'objet d'un audit.
- Dans le champ URL externe, vous pouvez spécifier l'adresse de l'application comme :
  - Adresse complète, incluant le nom de domaine complet ; par exemple :

    http://server1,mycompany.org/report/viewUserReport
  - Chemin relatif ; par exemple :

    /report/viewUserReport

    Si vous spécifiez le chemin relatif, Identity Manager ajoute automatiquement le nom de domaine complet du serveur sur lequel il est installé.
- Si vous le souhaitez, vous pouvez utiliser des objets gérés.
- Vous pouvez configurer des attributs à transmettre à l'URL.

  Spécifiez une URL pour l'application que vous voulez démarrer et incluez les attributs à transmettre à l'application.

Composants de tâches avancés

Les composants de tâches avancés permettent de spécifier un traitement personnalisé pour une tâche :

- La validation de niveau tâche valide une valeur d'attribut par rapport à d'autres attributs de la tâche. Par exemple, vous pouvez valider le fait que l'indicatif d'un numéro de téléphone spécifié par l'utilisateur corresponde au pays de l'utilisateur.
- Les gestionnaires de tâches métier (page 76) exécutent une logique métier personnalisée avant qu'une tâche Identity Manager ne soit soumise pour être traitée. En général, la logique métier personnalisée valide les données. Par exemple, un gestionnaire de tâches métier peut vérifier la limite d'appartenance d'un groupe avant qu'Identity Manager n'ajoute un nouveau membre au groupe. Si la limite d'appartenance du groupe est atteinte, le gestionnaire de tâches métier affiche un message indiquant à l'administrateur du groupe que le nouveau membre n'a pas pu être ajouté.

Création de gestionnaires de tâches métier

Pour définir le nom de classe complet d'un gestionnaire de tâches métier, procédez comme suit :

1. Créez ou modifiez une tâche d'administration.
2. Dans l'onglet Profil d'administration, cliquez sur Gestionnaires de tâches métier.

   La fenêtre Gestionnaires de tâches métier apparaît. Cette fenêtre répertorie les gestionnaires de tâches métier affectés à la tâche. Identity Manager exécute les gestionnaires dans l'ordre dans lequel ils apparaissent dans la liste.
3. Cliquez sur Ajouter.

   La fenêtre Détails de gestionnaires de tâches métier apparaît.

Utilisez la fenêtre Détails de gestionnaires de tâches métier pour définir les informations suivantes sur le gestionnaire de tâches métier que vous affectez à la tâche :

Nom

Nom que vous affectez au gestionnaire de tâches métier.

Description

Description facultative du gestionnaire de tâches métier.

Classe Java

Nom de classe complet du gestionnaire de tâches métier, si le gestionnaire est implémenté dans Java ; par exemple :

com.mycompany.MyJavaBLTH

Identity Manager s'attend à ce que le fichier de classe soit situé dans le répertoire racine spécifié pour les fichiers de classe Java personnalisés. Pour obtenir des informations sur le déploiement de fichiers de classe Java, reportez-vous au *Manuel de programmation Java*.

Nom du ficher JavaScript

Si le gestionnaire de tâches métier est implémenté dans JavaScript et que le code JavaScript est contenu dans un fichier, spécifiez le nom du fichier dans ce champ. Par exemple, vous pouvez placer le script Java dans un fichier si le gestionnaire de tâches métier doit être utilisé par plusieurs fenêtres de tâche.

Identity Manager s'attend à ce que le fichier de classe soit situé dans le répertoire racine spécifié pour les fichiers de classe Java personnalisés. Pour obtenir des informations sur le déploiement de fichiers de classe Java, reportez-vous au *Manuel de programmation Java*.

Si vous stockez le fichier dans un sous-répertoire de la racine, incluez le nom du sous-répertoire lorsque vous spécifiez le nom du fichier JavaScript ; par exemple :

JavaScriptSubDir\MyJavaScriptBLTH.js

Les barres obliques doivent correspondre à la plate-forme sur laquelle le fichier JavaScript est déployé.

JavaScript

Vous pouvez implémenter un gestionnaire de tâches métier JavaScript en tapant le code JavaScript complet dans ce champ plutôt que dans un fichier. Par exemple, vous pouvez placer le code JavaScript dans ce champ si le script est très court ou s'il doit être utilisé sans aucune autre fenêtre de tâche.

Propriété et Valeur

Avec les implémentations Java, ces champs sont des paires de données nom/valeur facultatives transmises à la méthode init() du gestionnaire de tâches métier Java, à utiliser de la manière requise par la logique métier du gestionnaire.

Pour ajouter une propriété définie par l'utilisateur, spécifiez un nom et une valeur de propriété, puis cliquez sur Ajouter.

Remarque : Si vous ajoutez un gestionnaire de tâches métier Java, le serveur d'applications du gestionnaire à charger redémarre.

Evénements et tâches d'administration

Les tâches d'administration incluent des *événements*, actions qu'CA IdentityMinder effectue pour réaliser la tâche. Une tâche peut inclure plusieurs événements. Par exemple, la tâche Créer un utilisateur peut inclure des événements qui créent le profil de l'utilisateur, ajoutent l'utilisateur à un groupe et affectent des rôles.

Identity Manager audite les événements, applique les règles métier spécifiques au client associées aux événements et requiert l'approbation des événements lorsque ces derniers sont mappés aux processus de flux de travaux.

Si plusieurs événements sont générés pour une tâche et qu'ils sont mappés à des processus de flux de travaux, ces derniers doivent être achevés pour qu'Identity Manager puisse exécuter la tâche.

Evénements principaux et secondaires

Les événements sont généralement indépendants des autres événements. Toutefois, certaines tâches sont associées à un événement principal et à un ou plusieurs événements secondaires.

- Un échec de l'événement principal provoque le rejet automatique de tous ses événements secondaires. Par exemple, si un événement CreateUserEvent échoue, il n'est pas nécessaire que l'événement AddToGroupEvent se produise pour l'utilisateur. Il entraîne également l'annulation de la tâche associée.
- Un échec d'un événement secondaire n'affecte pas la réussite ou l'échec de tout autre événement exécuté pour la tâche ou l'exécution de la tâche. Par exemple, dans la tâche Créer un utilisateur, un événement AddToGroupEvent peut être rejeté, ce qui signifie que le nouvel utilisateur ne peut pas être ajouté à un groupe. Il est toujours possible de créer l'utilisateur (CreateUserEvent), de l'affecter aux rôles de provisionnement (AssignProvisioningRoleEvent), voire même de l'ajouter à d'autres groupes.

Affichage des événements associés à une tâche

Vous pouvez afficher les événements associés à une tâche dans la console d'utilisateur CA IdentityMinder.

Pour afficher des événements associés à une tâche :

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Afficher la tâche d'administration.
2. Recherchez et sélectionnez la tâche appropriée.
3. Sélectionnez l'onglet Evénements.

   CA IdentityMinder affiche les événements associés à la tâche actuelle.

Evenements générés par les profils non modifiés

Les objets d'utilisateur, de groupe et d'organisation contiennent des attributs physiques qui sont stockés dans l'annuaire des utilisateurs. Si vous modifiez un attribut physique de l'un de ces objets dans un onglet de profil, Identity Manager génère un événement Modifier... une fois que l'utilisateur a envoyé la tâche. Par exemple, si l'attribut *Titre* est modifié dans l'onglet Profil de l'utilisateur, Identity Manager génère l'événement ModifyUserEvent.

Si un objet d'utilisateur, de groupe ou d'organisation est représenté dans un onglet de profil mais qu'aucun attribut physique n'a été modifié lorsque l'utilisateur clique sur Soumettre, Identity Manager ne génère pas d'événement Modifier.... Il génère l'événement Afficher... correspondant, comme suit.

- ViewUserEvent est généré à la place de ModifyUserEvent
- ViewGroupEvent est généré à la place de ModifyGroupEvent
- ViewOrganizationEvent est généré à la place de ModifyOrganizationEvent

Traitement des tâches d'administration

La durée de traitement d'une tâche dépend des étapes impliquées. Lorsqu'une tâche est soumise pour être traitée, Identity Manager effectue les étapes suivantes :

1. Identity Manager valide les données soumises.

   Il s'agit de la *phase synchrone*.

2. Si la tâche nécessite d'être approuvée, Identity Manager l'envoie au moteur de flux de travaux.

   a. Le moteur de flux de travaux détermine les approbateurs et place la tâche d'approbation dans leurs listes de travail.

   b. Le cas échéant, Identity Manager envoie un courriel notifiant les approbateurs de la tâche en attente.

   c. Un approbateur réserve la tâche (ce qui la supprime des listes de travail des autres approbateurs), puis l'approuve ou la rejette.

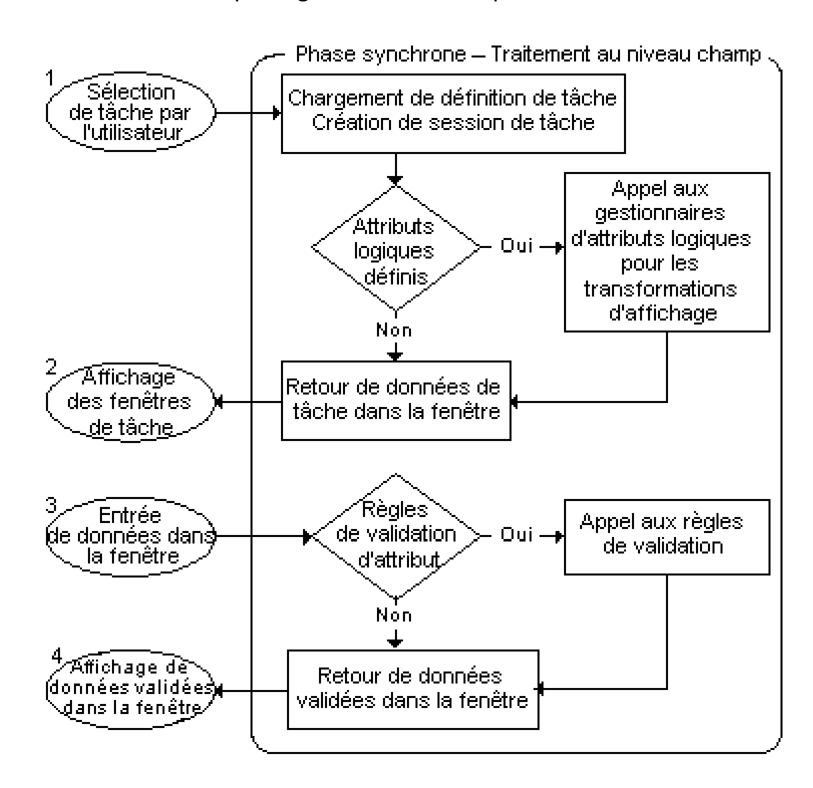
   d. Le cas échéant, Identity Manager envoie un courriel notifiant les utilisateurs impliqués du statut de la tâche.

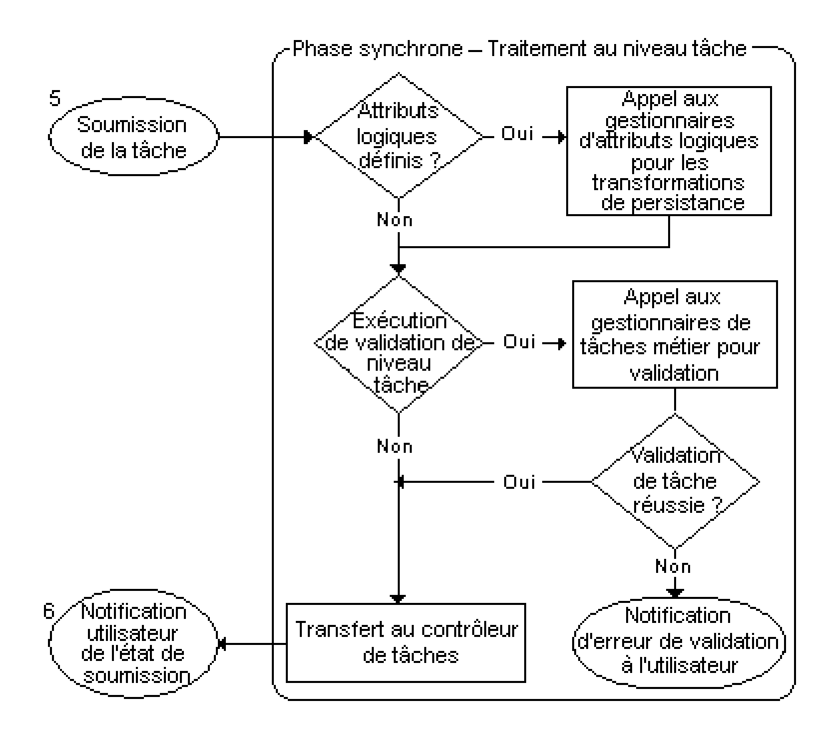
   Il s'agit de la *phase asynchrone*.

3. Identity Manager effectue la tâche, si elle n'a pas été rejetée.

Traitement de phase synchrone

Lors de la phase synchrone, Identity Manager peut transformer et valider les données que l'utilisateur entre dans les fenêtres de tâche, ainsi qu'appliquer la logique métier sur ces données avant que la tâche ne soit soumise pour traitement. Le diagramme suivant fournit une description générale de cette phase.

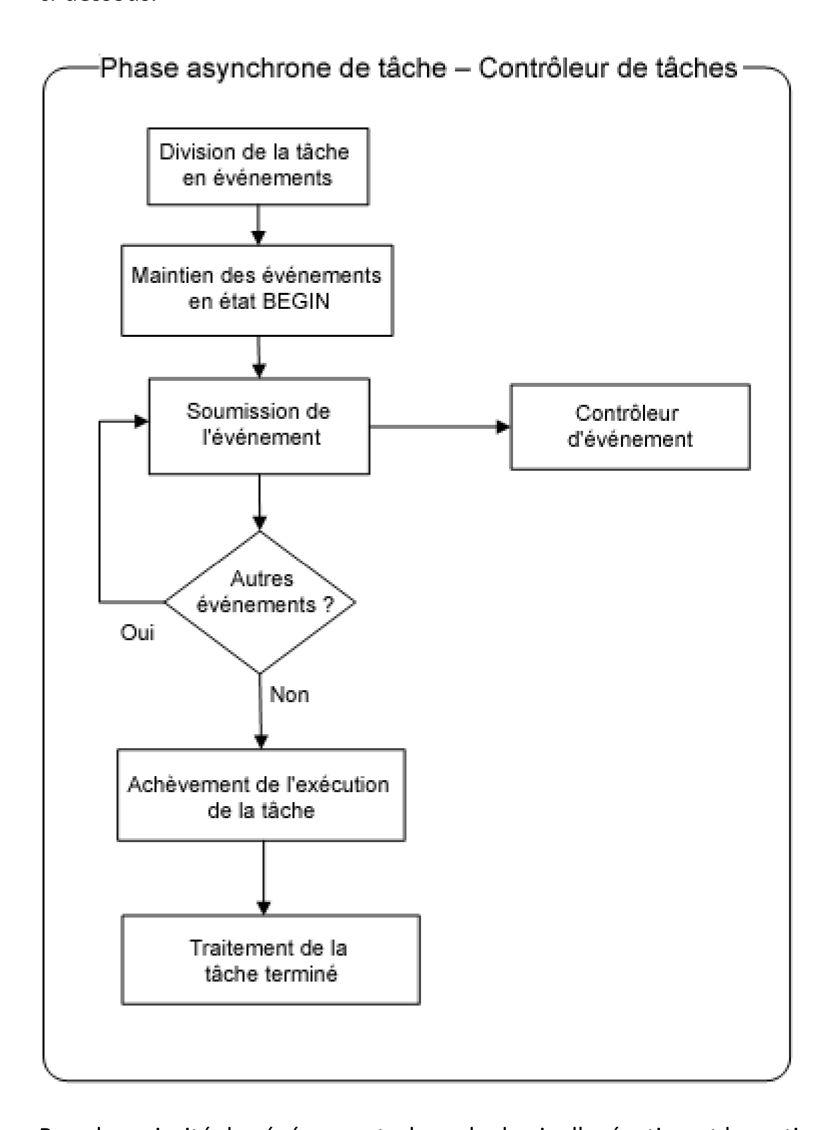




Traitement de phase asynchrone

A la fin de la phase synchrone, la tâche entre dans la phase asynchrone pour l'exécution. Au cours de cette phase, une tâche génère un ou plusieurs événements. Ceux-ci peuvent être définis par l'utilisateur (création d'un profil d'utilisateur, ajout d'un utilisateur à un groupe, etc.) ou générés par le système (enregistrement d'informations dans le journal d'audit).

Le contrôleur de tâches, un composant du serveur Identity Manager, est responsable du cycle de vie d'une tâche et de ses événements, comme indiqué dans l'illustration ci-dessous.



Pour la majorité des événements, le cycle de vie, l'exécution et les actions sont indépendantes des autres événements. Les tâches de création nécessitent que l'événement de création de l'objet principal s'exécute avant les événements secondaires.

Un événement présente généralement les états suivants.

- Début
- En attente
- Approuvé
- Exécuter
- Terminé
- Validé

Remarque : Identity Manager inclut des points d'insertion, appelés EventListeners, qui "écoutent" un événement ou un groupe d'événements. Lorsque l'événement se produit, l'écouteur d'événements applique une logique métier personnalisée adaptée à l'événement et à son état actuel. L'API Ecouteur d'événements permet d'enregistrer des écouteurs d'événements personnalisés. Pour plus d'informations, reportez-vous au *manuel de programmation Java (en anglais)*.

Images destinées à des tâches d'administration

Vous pouvez créer des images à utiliser avec des tâches d'administration que vous avez placées dans la page d'accueil.

Chapitre 4: Utilisateurs

Ce chapitre traite des sujets suivants :

Création et configuration d'un utilisateur

Les profils d'utilisateur permettent aux administrateurs de gérer les informations d'utilisateur, les droits, les applications et l'accès aux services, et d'accorder des droits d'autogestion aux utilisateurs pour leurs propres comptes et services. La création de profils d'utilisateur est une tâche commune pour un administrateur système.

Lors de la création et de la configuration d'un utilisateur, tenez compte des éléments de compte d'utilisateur suivants :

Tâches d'auto-administration : les profils d'utilisateurs sont configurés par défaut pour accorder l'accès à certaines tâches d'auto-administration, telles que la modification des informations de mots de passe et de profil. Un administrateur système disposant des tâches appropriées peut modifier les tâches d'auto-administration accordées aux utilisateurs par défaut.

Groupes : les groupes simplifient la gestion des rôles. Par exemple, un administrateur système disposant des tâches appropriées peut configurer plusieurs rôles pour affecter automatiquement le système à un utilisateur qui est ajouté en tant que membre d'un groupe.

Rôles d'administration : les rôles d'administration définissent les tâches qu'un utilisateur peut effectuer dans la console d'utilisateur. Par exemple, une tâche peut permettre à un utilisateur de modifier des informations de compte d'utilisateur, telles que l'adresse ou le poste. Une autre tâche peut permettre à un utilisateur d'administrer des tâches, telles que l'octroi d'une appartenance d'utilisateur à un groupe. Lorsque vous affectez un rôle d'administration à un utilisateur, l'utilisateur peut effectuer les tâches associées au rôle.

Comptes du terminal et Rôles de provisionnement : les comptes qui existent sur d'autres systèmes sont nommés Comptes de terminaux. Vous pouvez affecter des comptes sur des terminaux à des utilisateurs CA Cloud Access Manager grâce aux rôles de provisionnement. Par exemple, un utilisateur a besoin d'un compte Exchange pour la messagerie électronique, d'un compte Oracle pour l'accès à la base de données et d'un compte Active Directory pour utiliser un système Windows. Lorsque vous affectez un rôle de provisionnement à un utilisateur, l'utilisateur reçoit les comptes de terminal que le rôle de provisionnement spécifie.

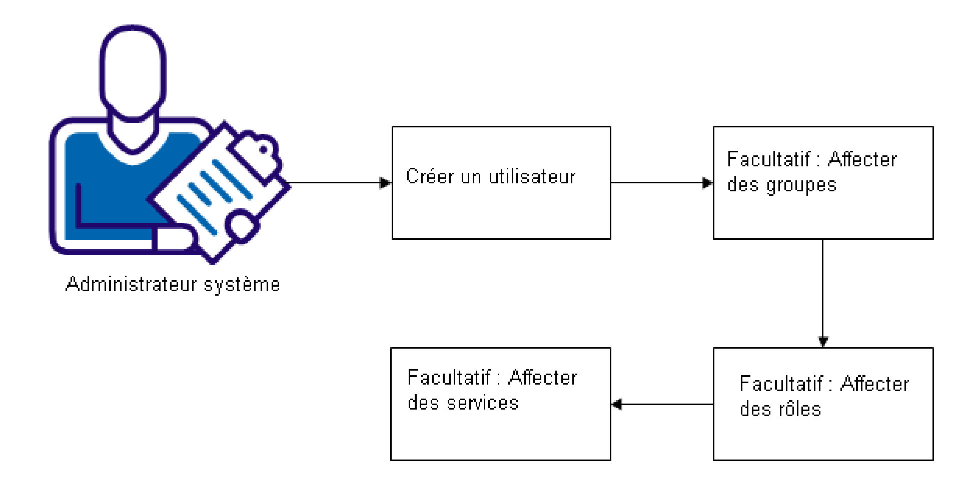
Rôles d'accès : les rôles d'accès permettent de fournir des droits dans CA IdentityMinder ou une autre application. Par exemple, vous pouvez utiliser les rôles d'accès pour effectuer les tâches suivantes :

- Fournir l'accès indirect à un attribut d'utilisateur
- Créer des expressions complexes
- Définir un attribut dans un profil d'utilisateur, qui est utilisé par une autre application pour définir des droits

Services : les services vous permettent de combiner des tâches d'utilisateur, des rôles, des groupes et des attributs dans un package unique. Vous pouvez gérer cet ensemble de droits de manière groupée. Par exemple, un nouvel employé des ventes a besoin d'un accès à un ensemble défini de tâches, de comptes sur des systèmes d'extrémité spécifiques et d'informations ajoutées à son profil de compte d'utilisateur. Lorsque vous affectez un service à un utilisateur, l'utilisateur reçoit l'ensemble entier de rôles, de tâches, de groupes et d'attributs de compte que le service spécifie.

Stratégies de mots de passe : les stratégies permettent de gérer les mots de passe des utilisateurs en appliquant des règles et des restrictions qui régissent l'expiration, la composition et l'utilisation des mots de passe. Si un administrateur système a créé des stratégies de mot de passe pour votre environnement, ces stratégies sont appliquées automatiquement aux nouveaux utilisateurs correspondant à une ou plusieurs règles de stratégies de mot de passe. Un administrateur système disposant des tâches appropriées peut modifier des stratégies de mot de passe.

Le schéma suivant contient des informations importantes et les étapes à suivre pour la création et la configuration d'un utilisateur.



Les rubriques suivantes décrivent de manière détaillée la procédure de création et de configuration des utilisateurs.

1. Création d'un utilisateur
2. Affectation à des groupes (page 88) (si nécessaire)
3. Affectation d'un rôle à un utilisateur (si nécessaire)
4. Affectation de services (page 89) (si nécessaire)

Création et configuration d'un utilisateur

Utilisez cette procédure pour créer un profil d'utilisateur. Selon la configuration de la tâche Créer un utilisateur, vous pourrez également utiliser cette tâche pour définir des éléments de profil supplémentaires. Vous pouvez ajouter un utilisateur à un groupe ou définir l'utilisateur en tant que membre d'un rôle de provisionnement ou d'administration.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur avec des tâches de gestion d'utilisateur.

   Le rôle Gestionnaire d'utilisateurs par défaut accorde les tâches appropriées.

2. Sélectionnez Utilisateurs, Gérer les utilisateurs, Créer un utilisateur.

   La tâche Créer un utilisateur apparaît.

3. Remplissez les champs d'informations de profil d'utilisateur, si nécessaire.
4. Cliquez sur Suivant.
5. Remplissez les champs dans les autres onglets de la tâche, le cas échéant.

   Par exemple, ajoutez l'utilisateur à un groupe ou affectez un rôle d'administration, un rôle de provisionnement ou le service à l'utilisateur, si ces options sont disponibles.
6. Cliquez sur Terminer.

   L'utilisateur est créé.

Affectation d'un groupe à un utilisateur

Vous pouvez ajouter un utilisateur à un groupe en tant que membre.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur avec des tâches de gestion d'utilisateur.

   Remarque : Le rôle Gestionnaire d'utilisateurs par défaut accorde les tâches appropriées. Généralement, un administrateur de système ou de clients hébergés dispose de ce rôle par défaut.
2. Sélectionnez Groupes, puis Modifier des membres de groupe.

   La liste des groupes que vous pouvez gérer s'affiche.
3. Sélectionnez un groupe et cliquez sur Sélectionner.

   La liste des utilisateurs affectés au groupe s'affiche.
4. Cliquez sur Ajouter un utilisateur
5. Recherchez un utilisateur auquel vous voulez affecter le groupe.

   Pour afficher une liste de tous les utilisateurs pour lesquels vous avez des droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.
6. Sélectionnez un utilisateur et cliquez sur Sélectionner.

   Une liste mise à jour des utilisateurs affectés au groupe s'affiche.
7. Cliquez sur Soumettre.

   L'utilisateur spécifié devient membre du groupe.

Affectation d'un rôle à un utilisateur

Vous pouvez affecter des rôles de provisionnement à un utilisateur individuel.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur en tant qu'utilisateur avec la tâche Modifier les membres/administrateurs avec rôle de provisionnement.
2. Sélectionnez Rôles et tâches.
3. Sélectionnez l'une des tâches suivantes :
   - Rôles d'administration, Modifier les membres/administrateurs avec rôle d'administration
   - Rôles de provisionnement, Modifier les membres/administrateurs avec rôle de provisionnement
   - Rôles d'accès, Modifier les membres/administrateurs avec rôle d'accès

   Une fenêtre de recherche apparaît.
4. Sélectionnez le rôle que vous souhaitez affecter à l'utilisateur.

   L'onglet Appartenance s'ouvre.
5. Cliquez sur Ajouter un utilisateur.
6. Recherchez un utilisateur auquel vous voulez affecter le rôle.

   Pour afficher la liste de tous les utilisateurs pour lesquels vous disposez de droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.
7. Sélectionnez un utilisateur et cliquez sur Sélectionner.
8. Cliquez sur Soumettre.

   Les rôles spécifiés sont affectés à l'utilisateur.

Affectation d'un service à un utilisateur

Vous pouvez affecter un service directement à un utilisateur en particulier. Cet utilisateur devient *membre* du service.

Procédez comme suit:

1. A partir du menu de navigation, sélectionnez Services, Demander et afficher un accès.

   Une liste des services que vous pouvez administrer s'affiche.
2. Sélectionnez le service que vous voulez affecter à l'utilisateur, puis cliquez sur Sélectionner.

   Une liste d'utilisateurs affectés au service s'affiche.
3. Cliquez sur Demander l'accès.

4. Recherchez un utilisateur auquel vous voulez affecter le service.

   Pour afficher une liste de tous les utilisateurs pour lesquels vous avez des droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.

5. Sélectionnez un utilisateur et cliquez sur Sélectionner.

   Une liste mise à jour des utilisateurs affectés au service s'affiche.

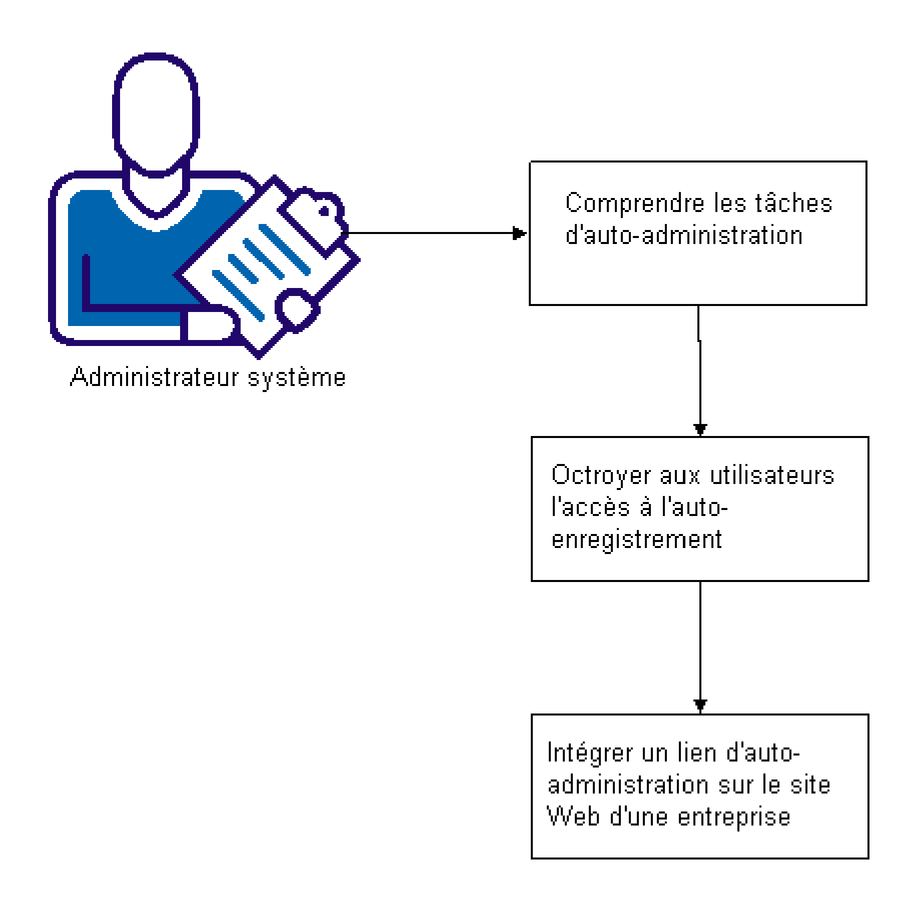
6. Cliquez sur Enregistrer les modifications.

   L'utilisateur reçoit le service spécifié. L'utilisateur reçoit toutes les applications, tous les rôles, tous les groupes et tous les attributs associés au service.

Octroi du droit d'auto-enregistrement aux utilisateurs

Les tâches d'auto-administration permettent aux utilisateurs de gérer eux-mêmes leur environnement. La tâche d'auto-enregistrement permet aux utilisateurs de créer leur propre compte d'utilisateur et leur profil à partir d'une console d'utilisateur publiquement disponible. Par exemple, Bentley Cola permet aux nouveaux employés et aux clients de créer leur propre compte d'utilisateur et leur profil grâce à un lien intégré sur le site Web de la société Bentley Cola.

Le schéma suivant contient des informations importantes et les étapes à suivre pour autoriser les utilisateurs à s'auto-enregistrer.



Les rubriques suivantes fournissent des détails sur la procédure à suivre pour octroyer le droit d'auto-enregistrement aux utilisateurs.

1. Description des tâches d'auto-administration (page 92)
2. Octroi de droits d'auto-enregistrement (page 93)
3. Intégration d'un lien d'auto-administration sur le site Web d'une société (page 93)

Tâches d'auto-administration

Les tâches d'auto-administration sont des actions entreprises par les utilisateurs, généralement à travers la console d'utilisateur, dans le but de gérer leurs profils. Les comptes d'utilisateurs sont configurés par défaut de sorte à accorder l'accès à certaines tâches d'auto-administration, telles que la modification des informations de mots de passe et de profil. Un administrateur système disposant des droits appropriés peut modifier les tâches d'auto-administration accordées aux utilisateurs par défaut.

Ces tâches d'auto-administration sont divisées en deux types :

- Tâches publiques : tâches auxquelles l'utilisateur peut accéder sans fournir de données de connexion. Par exemple, il peut s'agir de tâches d'auto-enregistrement, de mot de passe oublié ou d'ID d'utilisateur oublié.
- Tâches protégées : tâches pour lesquelles l'utilisateur fournit des données de connexion valides. Par exemple, il peut s'agir de tâches de modification de mot de passe ou d'informations de profils.

Le tableau suivant répertorie les tâches d'auto-administration par défaut.

Type de tâche	Tâches
Tâche publique	■ Auto-enregistrement : permet à l'utilisateur de s'enregistrer sur un site Web d'entreprise. ■ Réinitialisation du mot de passe oublié : permet à l'utilisateur de réinitialiser un mot de passe oublié. ■ Mot de passe oublié : affiche un mot de passe provisoire qui permet à l'utilisateur de se connecter à CA IdentityMinder. Lorsque l'utilisateur se connecte, il est invité à entrer un nouveau mot de passe. ■ ID d'utilisateur oublié : extrait ou réinitialise un ID d'utilisateur oublié.
Tâche protégée	■ Demander et afficher un accès : cette option permet aux utilisateurs de demander ou de supprimer l'accès aux services. ■ Modifier mon mot de passe : permet à l'utilisateur de réinitialiser son mot de passe. ■ Modifier mon profil : conserve les informations de profils, telles que les adresses et les numéros de téléphone. ■ Modifier mes groupes : permet à l'utilisateur de s'inscrire à des groupes. ■ Afficher mes rôles : affiche les rôles d'un utilisateur. ■ Afficher mes tâches soumises : affiche les tâches CA IdentityMinder lancées par l'utilisateur.

Accès aux tâches d'auto-administration

Après avoir configuré les tâches d'auto-administration pour votre environnement, vous pouvez ajouter les URL associées au site Web d'une entreprise.

Les URL d'auto-administration sont au format suivant :

https://*domaine*/iam/im/*alias_public*/ui7/index.jsp?task.tag=*balise_tâche*

Où :

- *domaine* correspond au nom de domaine complet du serveur Web dans l'environnement d'exécution de CA Cloud Access Manager.
- *alias* correspond à l'alias public de l'environnement. L'administrateur système définit l'alias public lors de la création de l'environnement.
- *balise_tâche* correspond à l'ID unique de la tâche.

  Pour la tâche Réinitialisation du mot de passe par défaut oublié, la balise de tâche est
  ForgottenPasswordReset.

  https://*domaine*/iam/im/*alias_public*/ui7/index.jsp?task.tag=ForgottenPasswordReset

  Pour la tâche ID utilisateur par défaut oublié, la balise de tâche est ForgottenUserID :

  https://*domaine*/iam/im/*alias_public*/ui7/index.jsp?task.tag=ForgottenUserID

Intégration d'un lien d'auto-administration sur le site Web d'une société

Pour permettre l'accès à une tâche d'auto-administration publique à partir du site Web d'une société, vous pouvez ajouter un lien à une page Web. Lorsqu'un utilisateur clique sur le lien, une fenêtre de tâche s'ouvre. Lorsque l'utilisateur termine la tâche, il est redirigé vers la console d'utilisateur par défaut.

Pour changer la page vers laquelle les utilisateurs sont redirigés, vous pouvez ajouter la balise task.RedirectURL à l'URL associée au lien comme suit :

<A href="http://*domaine*/iam/im/*alias_public*/ui7/index.jsp?task.tag=*balise_tâche*&task.RedirectURL=http://*domaine*/*URL_redirection*">*texte du lien*</A>

domaine

Nom de domaine complet du serveur Web dans l'environnement d'exécution de CA IdentityMinder.

alias_public

Chaîne unique ajoutée à l'URL pour l'accès aux tâches publiques.

Les tâches publiques sont des tâches d'auto-administration, telles que les tâches d'auto-enregistrement ou de mot de passe oublié. Les utilisateurs n'ont pas besoin de se connecter pour accéder à des tâches publiques.

Remarque : Pour plus d'informations sur les tâches et les alias publics, reportez-vous au manuel *Configuration Guide*.

balise_tâche

Identificateur unique de la tâche. Pour déterminer la balise de tâche, utilisez l'option Modifier la tâche d'administration pour afficher le profil pour la tâche.

URL_redirection

URL vers laquelle les utilisateurs sont redirigés après avoir soumis la tâche.

Par exemple, vous pouvez rediriger les utilisateurs vers une page d'accueil après leur auto-enregistrement.

texte du lien

Texte sur lequel les utilisateurs cliquent pour accéder à l'URL cible.

Par exemple, une société peut ajouter un lien permettant aux utilisateurs de réinitialiser un mot de passe oublié et de les rediriger ensuite vers une page d'accueil.

Le code HTML suivant représente un exemple de texte de lien :

<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/ index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://mon_serveur.ma_société.org/ welcome.html">Redéfinir le mot de passe</A>

Pour rediriger les utilisateurs vers la page grâce à laquelle ils ont pu accédé à la tâche d'auto-administration, spécifiez RefererURL comme valeur de balise pour task.RedirectURL comme suit :

<A href="http://*domaine*/iam/im/*alias_public*/ui7/index.jsp?task.tag=*balise_tâche*&task.RedirectURL=RefererURL</A>

Configuration de plusieurs tâches d'auto-administration

Vous pouvez créer plusieurs tâches d'auto-administration pour différents types d'utilisateurs. Par exemple, vous pouvez créer une tâche pour enregistrer de nouveaux employés et une autre tâche pour enregistrer des clients. A l'aide des tâches d'auto-enregistrement, vous pouvez effectuer les actions ci-après.

- Collecter différentes informations
- Enregistrer des utilisateurs dans différentes organisations
- Rediriger des utilisateurs vers différentes pages de déconnexion après leur enregistrement
- Utiliser différentes marques

Les figures ci-après illustrent la tâche d'auto-enregistrement pour de nouveaux employés et clients, respectivement.

Employé Auto-enregistrement

• = Obligatoire

Bienvenue à My company.com! Merci de joindre à notre équipe.

•Prénom

•Nom

•Sélectionner un mot de passe

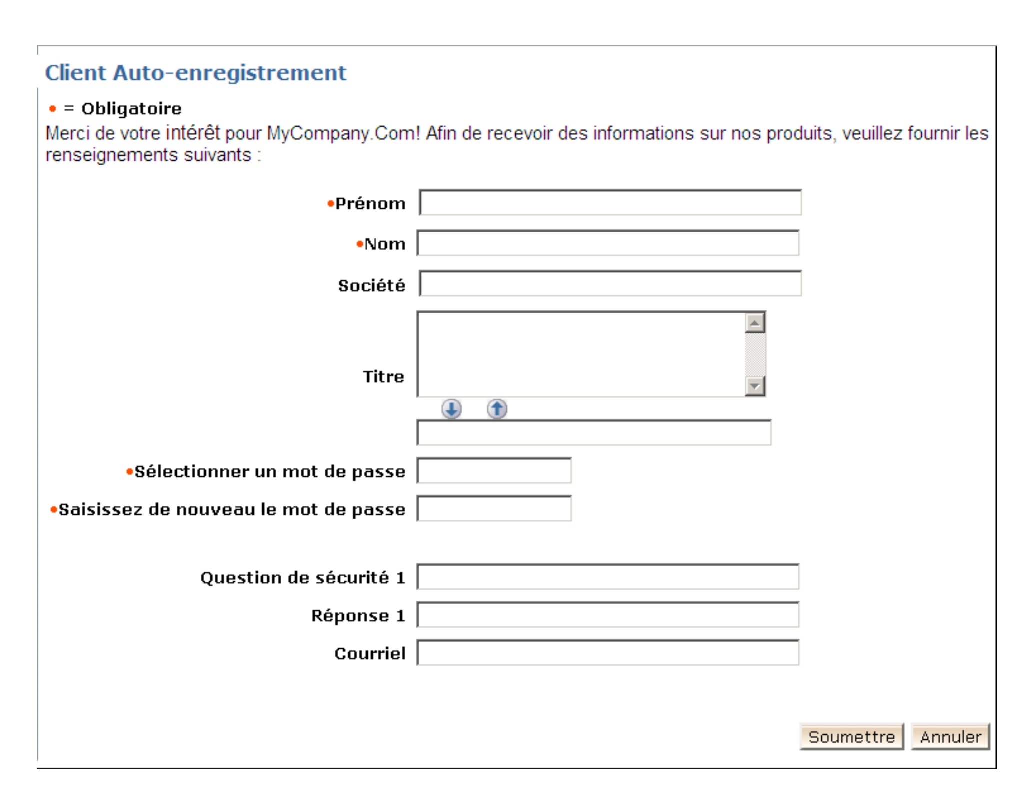
•Saisissez de nouveau le mot de passe

Question de sécurité 1

Réponse 1

Courriel

Soumettre Annuler



Pour configurer plusieurs tâches d'auto-administration du même type, indiquez une seule balise lorsque vous créez la tâche. Le champ Balise se trouve dans la fenêtre Configuration de profil pour la tâche.

Lorsque vous ajoutez le lien permettant d'accéder à la tâche sur un site Web, vous ajoutez la balise de la tâche, créant ainsi une URL unique.

Par exemple, vous pouvez créer deux tâches comme suit.

Tâche	Balise	URL
Enregistrer en tant que nouvel employé	Auto-enregistrement_employé	http://*domaine*/iam/im/*alias*/index.jsp?task.tag=Auto-enregistrement_employé
Enregistrer en tant que client	Auto-enregistrement_client	http://*domaine*/iam/im/*alias*/index.jsp?task.tag=Auto-enregistrement_client

Limitation de l'accès au rôle Auto-gestionnaire

Par défaut, le rôle Autogestionnaire, qui permet à l'utilisateur de gérer les informations de son profil et d'afficher ses rôles et tâches soumis, est affecté à tous les utilisateurs.

Pour attribuer le rôle d'auto-gestionnaire à un sous-ensemble d'utilisateurs, supprimez la stratégie de membre existante et créez une stratégie comme indiqué dans la section Définition des stratégies de membre pour un rôle d'administrateur.

Chapitre 5: Gestion des mots de passe

Ce chapitre traite des sujets suivants :

Gestion des mots de passe dans Identity Manager

Identity Manager comprend plusieurs fonctionnalités de gestion des mots de passe :

- Stratégies de mots de passe : ces stratégies gèrent les mots de passe utilisateur en appliquant des règles et restrictions qui régissent l'expiration, la composition et l'utilisation des mots de passe.
- Gestionnaires de mots de passe : les administrateurs qui ont le rôle de Gestionnaire de mots de passe peuvent réinitialiser un mot de passe lorsqu'un utilisateur appelle le Service d'assistance.
- Auto-administration de la gestion de mots de passe : Identity Manager comprend plusieurs tâches d'auto-administration qui permettent aux utilisateurs de gérer leurs propres mots de passe. Parmi ces tâches figurent notamment :
  - Auto-enregistrement : les utilisateurs indiquent un mot de passe lorsqu'ils s'enregistrent sur un site Web d'entreprise.
  - Modifier mon mot de passe : les utilisateurs peuvent modifier leurs mots de passe sans aide du personnel informatique ou du service d'assistance.
  - Mot de passe oublié : les utilisateurs peuvent réinitialiser ou récupérer un mot de passe oublié après vérification de leur identité par Identity Manager.
  - Réinitialiser le mot de passe ou Déverrouiller un compte (page 117): les utilisateurs peuvent réinitialiser ou récupérer un mot de passe oublié ou déverrouiller un compte sur le système lorsqu'ils accèdent à Identity Manager.
  - ID d'utilisateur oublié : les utilisateurs peuvent récupérer un ID oublié après vérification de leur identité par Identity Manager.
- Synchronisation des mots de passe sur les comptes de terminaux : les modifications de mot de passe sont synchronisées dans Identity Manager, le serveur de provisionnement et ses systèmes cibles. Les nouveaux mots de passe font l'objet d'une vérification par rapport aux stratégies de mots de passe d'Identity Manager.

Présentation de stratégies de mot de passe

Une stratégie de mot de passe est un ensemble de règles et restrictions. Ces règles spécifient la création et l'expiration de mots de passe. Lorsque vous configurez une stratégie de mots de passe dans un environnement CA IdentityMinder, elle s'applique au magasin d'utilisateurs associé à l'environnement. Si l'annuaire d'utilisateurs est associé à plusieurs environnements, une stratégie de mots de passe définie dans un environnement peut également s'appliquer dans d'autres environnements.

Dans une règle de mot de passe, vous pouvez configurer les paramètres suivants :

Remarque : Certains de ces paramètres requièrent des mappages d'annuaires d'utilisateurs pour certains attributs. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

- Application de mots de passe à un ensemble spécifique d'utilisateurs
- Expiration du mot de passe : définissez les événements qui entraînent l'expiration d'un mot de passe, tels qu'un délai écoulé ou un certain nombre d'échecs de connexion. Lorsqu'un mot de passe expire, le compte de l'utilisateur est désactivé.
- Composition du mot de passe : indique les exigences de contenu des nouveaux mots de passe. Par exemple, vous pouvez configurer des paramètres qui imposent aux utilisateurs de créer des mots de passe contenant au moins huit caractères, dont un chiffre et une lettre.
- Expressions régulières : fournit une expression déterminant le format d'un mot de passe valide. Vous pouvez indiquer si les mots de passe doivent correspondre à ce format. Vous pouvez également spécifier plusieurs expressions régulières.
- Restrictions du mot de passe : définissez les limites de réutilisation d'un mot de passe. Par exemple, les utilisateurs doivent attendre 90 jours avant de réutiliser un même mot de passe.
- Options avancées de mot de passe : indiquent les actions que CA IdentityMinder doit effectuer, telles que l'utilisation de caractères en minuscules, avant de traiter un mot de passe. Vous pouvez également indiquer la priorité d'une stratégie de mot de passe, si plusieurs stratégies de mot de passe s'appliquent.

Les utilisateurs de SiteMinder peuvent également configurer des stratégies de mots de passe dans l'interface administrative SiteMinder. Ces stratégies s'affichent dans la console d'utilisateur CA IdentityMinder.

Remarque : Lorsque CA IdentityMinder s'intègre à SiteMinder, SiteMinder applique *toutes* les stratégies de mot de passe.

Pour créer une stratégie de mot de passe :

Vous créez des stratégies de mot de passe à l'aide de la console d'utilisateur de CA IdentityMinder.

Remarque : Certaines options de stratégie de mot de passe seront disponibles uniquement si certains attributs connus sont mappés. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

Procédez comme suit:

1. Dans la console d'utilisateur, choisissez Stratégies, Gérer les stratégies de mot de passe, Créer une stratégie de mot de passe.
2. Saisissez un nom unique et une description (facultative) pour la stratégie de mots de passe.
3. Configurez ces paramètres de stratégie de mot de passe en fonction de votre implémentation :
   - Application d'une stratégie de mots de passe à un ensemble d'utilisateurs (page 102)
   - Configuration de l'expiration de mot de passe (page 104)
   - Configuration de la composition de mots de passe (page 108)
   - Spécification d'expressions régulières (page 110)
   - Définition de restrictions de mot de passe (page 112)
   - Configuration d'options avancées de mot de passe (page 115)

Activation de stratégies de mots de passe supplémentaires

CA IdentityMinder vous permet de créer des stratégies de mot de passe de base qui gèrent les mots de passe des utilisateurs en appliquant l'expiration de mot de passe, la composition et l'utilisation. Vous pouvez également définir ces règles de mot de passe supplémentaires et ces restrictions :

- Expiration du mot de passe :
  - Suivi des échecs de connexion ou des connexions établies
  - Authentification d'une connexion
  - Expiration du mot de passe s'il n'est pas modifié
  - Inactivité du mot de passe
  - Mot de passe incorrect
  - Plusieurs expressions régulières

- Restrictions de mot de passe :
  - Nombre minimum de jours avant la réutilisation
  - Nombre minimum de mots de passe avant la réutilisation
  - Pourcentage différent du dernier mot de passe
  - Omission de séquence lors de la vérification des différences

Procédez comme suit:

1. Accédez à Répertoires, <nom_répertoire>, Utilisateur dans la console de gestion.
2. Vérifiez que %PASSWORD DATA% et %ENABLED STATES% -> 'STATE' sont mappés vers des attributs physiques.
3. Ces attributs sont mappés par défaut dans les fichiers d'exemple directory.xml. Si ces attributs ne sont pas mappés, consultez le manuel *CA IdentityMinder Configuration Guide* pour plus d'informations.

Application d'une stratégie de mots de passe à un ensemble d'utilisateurs

Vous pouvez spécifier des règles qui déterminent l'ensemble d'utilisateurs auxquels une stratégie de mot de passe s'applique. Vous pouvez ainsi définir une stratégie de mots de passe pour les employés en général et une stratégie plus rigoureuse pour les managers principaux.

Procédez comme suit:

1. Créez ou modifiez une stratégie de mots de passe dans la console d'utilisateur.
2. Sélectionnez le type de filtre à configurer dans le champ Filtre d'annuaire.

   Reportez-vous au tableau suivant pour une description de chaque type de filtre.

   Remarque : Le type de référentiel d'utilisateurs auquel la stratégie de mot de passe s'applique détermine les options pour la zone de liste de filtres d'annuaire. Certains types de filtre ne sont pas disponibles pour des bases de données relationnelles et les référentiels d'utilisateurs CA Directory lorsque CA IdentityMinder est intégré à CA SiteMinder Web Access Manager.
3. Indiquez une condition en sélectionnant un attribut et un opérateur puis en saisissant une valeur.
4. Cliquez sur le signe plus pour ajouter des conditions supplémentaires.

Le tableau suivant décrit les options des types de filtres d'annuaire et donne des exemples pour chacun d'entre eux. Les attributs sur le côté gauche du signe = dans les exemples suivants apparaissent tels qu'ils sont définis dans la zone de définition de l'annuaire de l'utilisateur. Pour des tâches de création d'utilisateur, les stratégies de mot de passe comprenant des filtres d'annuaires sont uniquement appliquées lorsque les deux conditions suivantes sont remplies :

- CA IdentityMinder n'est pas intégré à CA SiteMinder Web Access Manager.
- Le type de filtre d'annuaire n'est pas Utilisateur, Groupe, Filtre de groupe ou Recherche de groupe.

Type de filtre	Utiliser ce filtre pour...	Exemple
Dans une organisation	Recherchez et sélectionnez une organisation.	
Dans un groupe	Recherchez et sélectionnez un groupe.	
Un utilisateur	Recherchez et sélectionnez un utilisateur unique.	
Filtre d'utilisateur (Non disponible pour les bases de données relationnelles en cas d'intégration à CA SiteMinder Web Access Manager)	Spécifier un filtre pour des utilisateurs.	Type d'employé = Sous-traitant Département = Sécurité
Expression de recherche d'utilisateurs	Saisir une requête de recherche pour des utilisateurs.	uid=jsmith (pour LDAP) TBLUSERS.ID = jsmith (pour des bases de données relationnelles)
Filtre de groupe (Non disponible pour les bases de données relationnelles en cas d'intégration à CA SiteMinder Web Access Manager)	Spécifier un filtre pour des groupes.	Auto-abonnement = *
Expression de recherche de groupes	Saisir une requête de recherche pour des groupes.	cn=Sales (pour LDAP) TBLGROUPS.NAME=GroupA (pour des bases de données relationnelles)

Type de filtre	Utiliser ce filtre pour...	Exemple
Filtre d'organisations (Non disponible pour les bases de données relationnelles en cas d'intégration à CA SiteMinder Web Access Manager)	Spécifier un filtre pour des organisations.	Nom d'organisation = *Marketing
Expression de recherche d'organisations	Saisir une requête de recherche pour des organisations.	ou=Boston (pour LDAP) TBLORGANIZATIONS.NAME=Boston (pour des bases de données relationnelles)
rechercher	Indiquez une requête non comprise dans les autres options de type de filtre.	(&(ID unique=*smith)(ou=Boston))

Configuration de l'expiration de mot de passe

Pour aider à gérer l'accès utilisateur, vous pouvez définir des événements tels que plusieurs échecs de connexion ou l'inactivité de compte. Lorsque ces événements se produisent, CA IdentityMinder désactive le responsable du compte d'utilisateur. Lorsque CA IdentityMinder est intégré à SiteMinder, vous pouvez spécifier une redirection.

Remarque : Ces paramètres requièrent une configuration supplémentaire. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

Vous pouvez configurer les paramètres suivants pour l'expiration de mot de passe :

- Case à cocher Suivi des connexions réussies/Suivi des échecs de connexion
- Case à cocher Authentifier en cas d'échec du suivi des connexions
- Paramètres de modification de mot de passe pour éviter son expiration
- Paramètres d'expiration de mot de passe en cas d'inactivité
- Paramètres de mot de passe incorrects

Case à cocher Suivi des connexions réussies/Suivi des échecs de connexion

Cette case à cocher active et désactive le suivi des tentatives de connexion d'utilisateur, y compris l'heure de la dernière tentative de connexion. Si vous activez cette case à cocher, CA IdentityMinder écrit des informations de connexion dans un attribut de données de mot de passe dans le magasin d'utilisateurs.

Remarque : Ce paramètre requiert une configuration supplémentaire. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

Lorsque la case à cocher Suivi des échecs de connexion est activée, la section Mot de passe incorrect et la case à cocher Authentifier en cas d'échec du suivi des connexions sont activées. Lorsque la case à cocher Suivi des connexions réussies est activée, la section Expiration du mot de passe en cas d’inactivité et la case à cocher Authentifier en cas d'échec du suivi des connexions sont activées.

Si vous disposez de plusieurs stratégies de mot de passe, assurez-vous que toutes les stratégies de mot de passe applicables désactivent les détails de connexion. Dans le cas contraire, une stratégie unique qui active le suivi de détails de connexion peut entraîner des erreurs de stratégies de mot de passe.

Case à cocher Authentifier en cas d'échec du suivi des connexions

Sélectionnez cette case à cocher pour activer les connexions en cas d'échec du suivi d'utilisateur. Par défaut, cette case à cocher est désactivée. Lorsque le suivi des connexions est désactivé, les utilisateurs ne peuvent pas se connecter.

Lorsque vous sélectionnez cette case à cocher, vous devez sélectionner également la case à cocher Suivi des échecs de connexion ou la case à cocher Suivi des connexions réussies.

Remarque : Ce paramètre requiert une configuration supplémentaire. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

Paramètres de modification de mot de passe pour éviter son expiration

Dans les champs Modification du mot de passe pour éviter son expiration, vous pouvez configurer le comportement des mots de passe ayant expiré. Vous pouvez également programmer l'envoi d'avertissements d'expiration de mot de passe aux utilisateurs.

Remarque : Ce paramètre requiert une configuration supplémentaire. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

Vous pouvez configurer les champs suivants :

Après *<nombre>* jours

Détermine le délai en jours après l'expiration d'un mot de passe avant la désactivation de l'utilisateur par CA IdentityMinder ou la modification du mot de passe.

Remarque : CA IdentityMinder désactive le compte d'utilisateur uniquement lorsque l'utilisateur tente de se connecter après expiration du délai.

Désactiver un utilisateur

Sélectionnez ce bouton radio pour désactiver l'utilisateur lorsque le mot de passe expire. Vous pouvez désactiver des utilisateurs à l'aide des éléments suivants :

- Tâche Activer/Désactiver un utilisateur dans la console d'utilisateur. (Les rôles Administrateur système, Gestionnaire d'organisations et Gestionnaire de la sécurité par défaut incluent la tâche Activer/Désactiver un utilisateur.)
- Interface d'administrateur CA SiteMinder Web Access Manager.

  Remarque : Pour plus d'informations, consultez le manuel *CA SiteMinder Web Access Manager Policy Server Administration Guide*.

Forcer la modification du mot de passe

Activez ce bouton radio pour modifier un mot de passe lors de la prochaine tentative de connexion de l'utilisateur.

Envoyer des avertissements d'expiration pour *<nombre>* jours

Entrez le délai en jours pour l'envoi de notifications avant l'expiration du mot de passe.

Paramètres d'expiration de mot de passe en cas d'inactivité

Les paramètres Expiration du mot de passe en cas d’inactivité vous permettent de spécifier l'intervalle de connexions de l'utilisateur. Une fois cet intervalle écoulé, le compte d'utilisateur est considéré comme inactif. Vous pouvez également utiliser cette section pour spécifier une action lorsqu'un utilisateur dont le compte est considéré inactif est autorisé à se connecter.

Pour configurer des paramètres dans la section Expiration du mot de passe en cas d’inactivité, vous devez activer les cases à cocher de détails de suivi des connexions.

Remarque : Ce paramètre requiert une configuration supplémentaire. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

La section Expiration du mot de passe en cas d’inactivité contient les paramètres suivants :

- Après *<nombre>* jours - Nombre de jours d'inactivité avant expiration du mot de passe expire.
- Désactiver un utilisateur - Désactive l'utilisateur lorsque le mot de passe expire en cas d'inactivité, le compte d'utilisateur est désactivé. Les utilisateurs désactivés doivent alors être activés à l'aide de la tâche Activer/Désactiver un utilisateur.
- Forcer la modification du mot de passe - Force la modification du mot de passe lorsqu'un mot de passe expire en cas d'inactivité. L'utilisateur modifie le mot de passe lors de la tentative de connexion suivante.

Paramètres de mot de passe incorrects

Dans la section Mot de passe incorrect, vous pouvez spécifier le nombre d'échecs de connexions autorisés avant la désactivation du compte d'utilisateur. Vous pouvez également spécifier le délai de désactivation de compte avant qu'un utilisateur puisse se connecter à nouveau. Cette section s'applique uniquement lorsque la case à cocher Suivi des échecs de connexion est activée.

Remarque : Ce paramètre requiert une configuration supplémentaire. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

La zone Mot de passe incorrect contient les champs suivants :

Compte désactivé après *<nombre>* mots de passe incorrects successifs

Ce paramètre détermine le nombre d'échecs de connexion consécutifs autorisés pour un utilisateur. La limitation du nombre de tentatives de connexion fournit une protection contre les programmes conçus pour accéder à une ressource par utilisation répétée de mots de passe de manière jusqu'à obtention du mot de passe correct. Si un utilisateur dépasse le nombre de tentatives de connexion spécifié, CA IdentityMinder désactive le compte. L'utilisateur devra contacter l'administrateur pour réactiver le compte.

Après *<nombre>* minutes

Ce paramètre détermine le délai d'attente d'un utilisateur avant la prochaine tentative de connexion ou la réactivation du compte. Si l'utilisateur entre un autre mot de passe incorrect, CA IdentityMinder désactive de nouveau le compte. L'utilisateur devra attendre l'écoulement de la durée spécifiée avant de tenter une nouvelle connexion.

Autoriser une tentative de connexion

Ce paramètre spécifie le délai en minutes suivant la saisie d'un mot de passe incorrect avant la prochaine tentative de connexion.

Réactiver le compte

Ce paramètre réactive un compte suite au délai spécifié en minutes.

Configuration de la composition de mots de passe

Vous pouvez spécifier des règles déterminant la composition des caractères des mots de passe nouvellement créés. Tenez compte de la longueur maximum des mots de passe avant de déterminer les valeurs requises pour les caractères. Si le nombre total de lettres et de nombres excède la longueur maximum définie, tous les mots de passe seront rejetés. Par exemple, si les lettres et les chiffres sont tous les deux définis sur six, tous les mots de passe contiendront au moins 12 caractères (6 lettres et 6 chiffres). Dans cet exemple, si la longueur de mot de passe maximum est de huit caractères, tous les mots de passe sont rejetés.

Les paramètres de composition de mot de passe incluent :

Longueur minimum du mot de passe

Spécifie la longueur minimum des mots de passe d'utilisateur.

Longueur maximum du mot de passe

Spécifie la longueur maximum des mots de passe d'utilisateur.

Nombre maximum de caractères répétés

Détermine le nombre maximum de caractères identiques qui peuvent s'afficher consécutivement dans un mot de passe.

Par exemple, si cette valeur est définie sur 3, alors aaaa ne peut apparaître nulle part dans le mot de passe. Toutefois, aaa sera accepté dans un mot de passe. Définissez cette valeur pour garantir que les utilisateurs ne peuvent pas entrer de mots de passe à caractères uniques.

Lettres majuscules

Spécifie si les lettres majuscules sont autorisées et, dans ce cas, le nombre minimum que le mot de passe devra contenir.

Minuscules

Spécifie si les lettres minuscules sont autorisées et, dans ce cas, le nombre minimum que le mot de passe devra contenir.

Lettres

Spécifie si l'utilisation de lettres est autorisée et, dans ce cas, le nombre minimum que le mot de passe devra contenir.

Remarque : La case à cocher Lettres est automatiquement sélectionnée lorsque vous autorisez l'utilisation de lettres majuscules ou minuscules.

Chiffres

Spécifie si l'utilisation de chiffres est autorisée et, dans ce cas, le nombre minimum que le mot de passe devra contenir.

Lettres et chiffres

Spécifie si l'utilisation de lettres et de chiffres est autorisée et, dans ce cas, le nombre minimum que le mot de passe devra contenir. Si ce paramètre est défini avec l'option Chiffres, les caractères pourront remplir les deux conditions. Par exemple, si ce paramètre et l'option Chiffres sont définis sur 4, le mot de passe 1234 sera un mot de passe valide.

Remarque : La case à cocher Lettres et chiffres est automatiquement sélectionnée lorsque vous autorisez l'utilisation de lettres majuscules ou minuscules ou de chiffres.

Ponctuation

Spécifie si l'utilisation de signes de ponctuation est autorisée et, dans ce cas, le nombre minimum que le mot de passe devra contenir. Les signes de ponctuation peuvent être des points, des virgules, des points d'exclamation, des barres obliques et des traits d'union.

Non imprimable

Spécifie si l'utilisation de caractères non imprimables est autorisée et, dans ce cas, le nombre minimum que le mot de passe devra contenir. Ces caractères ne s'affichent pas à l'écran.

Remarque : Certains navigateurs ne prennent pas en charge les caractères non imprimables.

Non alphanumérique

Spécifie si les caractères non alphanumériques peuvent être utilisés tels que les signes de ponctuation et d'autres symboles (@, $ et *) et dans ce cas, le nombre minimum qu'un mot de passe peut contenir. Les caractères non imprimables sont également inclus. Un caractère non alphanumérique remplit également les conditions des options Ponctuation et Non imprimable.

Spécification d'expressions régulières

Les expressions régulières de mot de passe permettent de spécifier des modèles de texte d'expressions régulières pour la mise en correspondance et la validation de chaînes de mot de passe. Ce test permet de requérir l'utilisation d'un chiffre en tant que caractère de début et d'un autre type de caractère de fin.

Vous pouvez configurer plusieurs expressions pour une stratégie de mot de passe unique. Si vous créez plusieurs expressions, les mots de passe acceptables devront correspondre à *toutes* les expressions spécifiées.

Procédez comme suit:

1. Saisissez une balise descriptive pour l'expression (sans espaces) dans le champ Nom.
2. Saisissez une expression régulière à l'aide de la syntaxe décrite dans la syntaxe d'expressions régulières du champ Doit correspondre.
3. Si le mot de passe ne correspond pas à l'expression régulière, sélectionnez la case à cocher dans la colonne Ne doit pas correspondre.

Remarque : Vous pouvez spécifier plusieurs expressions en cliquant sur le plus (+) pour ajouter l'expression.

Exemple : Vous pouvez utiliser la définition d'expression régulière suivante pour rechercher tous les mots de passe commençant par un caractère en majuscule ou en minuscule :Name : MustStartAlpha

Expression : [a-zA-Z].*

Syntaxe d'expressions régulières

Cette section décrit la syntaxe à utiliser pour créer des expressions régulières pour la correspondance de mots de passe. Cette syntaxe correspond à la syntaxe d'expression régulière prise en charge pour la correspondance de ressources lors de la spécification de domaines.

Caractères	Résultats
\	Utilisé pour mentionner un métacaractère (comme *)
\\	Correspond à un caractère \ unique
(A)	Sous-expressions de groupes (affecte l'ordre d'évaluation des modèles)

Caractères	**Résultats**
[abc]	Classe de caractères simples (un caractère entre crochets correspond au caractère cible)
[a-zA-Z]	Classe de caractère avec des plages (une plage de caractères entre crochets correspond au caractère cible)
[^abc]	Classe de caractères niés
.	Représente tout caractère autre que l'introduction d'une nouvelle ligne
^	Représente uniquement le début d'une ligne
$	Représente uniquement la fin d'une ligne
A*	Représente la lettre A, apparaissant 0 fois ou plusieurs fois (correspondance maximale)
A+	Représente la lettre A, apparaissant 1 fois ou plusieurs fois (correspondance maximale)
A?	Représente la lettre A, apparaissant 1 ou 0 fois (correspondance maximale)
A*?	Représente la lettre A, apparaissant 0 fois ou plusieurs fois (correspondance minimale)
A+?	Représente la lettre A, apparaissant 1 fois ou plusieurs fois (correspondance minimale)
A??	Représente la lettre A, apparaissant 0 ou 1 fois (correspondance minimale)
AB	Représente la lettre A suivie de la lettre B
A|B	Représente A ou B.
\1	Référence arrière à la première sous-expression entre parenthèses
\n	Référence arrière à la *n*ème sous-expression entre parenthèses

Tous les opérateurs de fermeture (+, *, ?) impliquent une correspondance maximale par défaut, c'est-à-dire qu'ils correspondent à autant d'éléments de la chaîne que possible sans faire échouer la correspondance globale. Si vous voulez utiliser un type de fermeture minimale (non maximale), ajoutez un ? juste après. Une fermeture minimale recherchera le moins d'éléments possible.

Définition de restrictions de mot de passe

Vous pouvez définir des restrictions sur l'utilisation de mot de passe. Les restrictions incluent le délai qu'un utilisateur doit patienter avant de réutiliser un mot de passe et le degré de différence du mot de passe par rapport aux mots de passe préalablement sélectionnés. Vous pouvez également empêcher les utilisateurs de spécifier des mots de passe pouvant représenter un risque pour la sécurité ou contenant des informations personnelles.

Remarque : Ce paramètre requiert une configuration supplémentaire. Consultez la section Activation de stratégies de mots de passe supplémentaires (page 101).

La section Restriction inclut les champs suivants :

Nombre minimum de jours avant la réutilisation

Détermine le délai en jours avant qu'un utilisateur puissent réutiliser un mot de passe.

Nombre minimum de mots de passe avant la réutilisation

Détermine le nombre de mots de passe qui doivent être utilisés avant de pouvoir réutiliser un mot de passe.

Remarque : Si vous spécifiez une durée et un nombre de mots de passe, les deux critères doivent être remplis avant de pouvoir réutiliser un mot de passe. Par exemple, vous pouvez configurer une stratégie de mot de passe qui requiert aux utilisateurs de patienter 365 jours et de spécifier 12 mots de passe avant de pouvoir réutiliser un mot de passe. Au bout d'un an, si seulement six mots de passe ont été utilisés, six autres mots de passe sont utilisés avant que l'utilisateur puisse réutiliser le premier mot de passe.

Pourcentage de différence par rapport au dernier mot de passe

Spécifie le pourcentage de correspondance d'un nouveau mot de passe. Vous pouvez définir la valeur sur 100. Dans ce cas, le nouveau mot de passe ne peut pas contenir de caractères ayant été utilisés dans le mot de passe précédent.

Ignorer la séquence lors de la vérification des différences

Ignore la position des caractères dans le mot de passe en cas de définition de pourcentage.

Par exemple, si le mot de passe initial est BASEBALL12 et que la case à cocher Ignorer la séquence lors de la vérification des différences est activée, 12BASEBALL n'est pas acceptable. Si vous désactivez la case à cocher, le mot de passe 12BASEBALL sera passe acceptable, car chaque lettre apparaît à une position différente.

Pour plus de sécurité, la case à cocher Ignorer la séquence lors de la vérification des différences est sélectionnée.

Mots de passe	Différence (%)	Ignorer la séquence	Accepté
BASEBALL12 (ancien) 12BASEBALL	0	Sélectionné Désélectionné	Oui Oui
BASEBALL12 (ancien) 12BASEBALL	100	Sélectionné Désélectionné	Non Oui
BASEBALL12 (ancien) 12SOFTBALL	0	Sélectionné Désélectionné	Oui Oui
BASEBALL12 (ancien) 12SOFTBALL	90	Sélectionné Désélectionné	Non Oui
BASEBALL12 (ancien) 12SOFTBALL	100	Sélectionné Désélectionné	Non Non

Attributs du profil

Configurez le champ Longueur de correspondance pour empêcher les utilisateurs d'utiliser des informations personnelles dans leurs mots de passe. Le champ Longueur de correspondance détermine la longueur de séquence minimum que la stratégie de mot de passe compare aux attributs dans l'entrée de l'annuaire. Par exemple, si cette valeur est définie sur quatre, CA IdentityMinder vérifie que le mot de passe n'inclut pas les quatre derniers caractères des attributs de profil d'utilisateur, par exemple, un nom de famille ou un numéro de téléphone.

Dictionnaire

Spécifie une liste de chaînes que vous ne pouvez pas utiliser dans des mots de passe.

Remarque : Un retour chariot est introduit après la dernière entrée du dictionnaire.

Les paramètres de dictionnaire incluent les champs suivants :

- Chemin d'accès : contient le chemin complet et le nom du fichier de dictionnaire.
- Longueur de correspondance : contrôle la longueur des chaînes comparées aux valeurs dans le fichier de dictionnaire. La comparaison ignore la casse des chaînes. Vous pouvez laisser le champ Longueur de correspondance vide ou le définir sur zéro. Dans ces cas, CA IdentityMinder rejette uniquement les mots de passe qui correspondent exactement à une chaîne dans le dictionnaire. Lorsque la longueur de correspondance est supérieure à zéro, CA IdentityMinder rejette les entrées dans les cas suivants :
  - Le mot de passe inclut une sous-chaîne qui commence par la même série de caractères qu'une entrée du dictionnaire.
  - Le nombre de caractères consécutifs correspondants est supérieur ou égal au nombre spécifié dans le champ Longueur de correspondance.

  Par exemple, si un fichier de dictionnaire contient les entrées suivantes :

  - lion
  - sites
  - ours

  Lorsque le champ Longueur de correspondance est défini sur quatre, les actions suivantes se produisent :

  "PetitOurs" est rejeté, car Ours correspond à l'entrée ours du fichier de dictionnaire.

  "visiter" est rejeté, car site correspond aux quatre premiers caractères de l'entrée site du fichier de dictionnaire.

  "truites" est accepté, car "ites" n'inclut pas la première lettre de l'entrée sites du fichier de dictionnaire.

Configuration d'options avancées de mot de passe

Les options de stratégie de mot de passe avancées permettent de configurer le prétraitement des mots de passe soumis avant la validation et le stockage. Vous pouvez également affecter à la stratégie une priorité pour permettre l'évaluation prévisible de plusieurs stratégies de mots de passe qui s'appliquent au même annuaire d'utilisateurs ou au même espace de noms.

Ne pas forcer la casse | Forcer les majuscules | Forcer les minuscules

Indiquez si les mots de passe doivent utiliser des majuscules ou des minuscules avant le traitement et le stockage. Choisissez une de ces options en cliquant sur le bouton radio Forcer les majuscules ou Forcer les minuscules. Dans le cas contraire, assurez-vous que le bouton radio Ne pas forcer la casse (valeur par défaut) est sélectionné.

Important : Vérifiez que l'option spécifiée imposant le type de casse est identique aux conditions de composition liée à la casse que vous avez définies.

Supprimer les espaces de début

Sélectionnez cette option pour supprimer l'espace en début de mot de passe avant le traitement.

Supprimer les espaces de fin

Sélectionnez cette option pour supprimer l'espace en fin de mot de passe avant le traitement.

Supprimer les espaces incorporés

Sélectionnez cette option pour supprimer les espaces dans le mot de passe avant le traitement.

Remarque : Certaines implémentations d'annuaires d'utilisateurs enlèvent automatiquement les espaces situés au début et à la fin des valeurs d'attribut (dans lesquelles les mots de passe d'utilisateur sont stockés) avant leur stockage. Les paramètres que vous spécifiez dans la stratégie de mot de passe n'ont aucun effet.

Priorité d'évaluation

Spécifie la priorité d'évaluation pour la stratégie de mot de passe. La valeur est comprise dans la plage 0 (valeur par défaut) à 999. Les stratégies applicables sont évaluées dans l'ordre décroissant (de 999 à 0).

Appliquer des stratégies de mot de passe de priorité inférieure

Cette option détermine si des stratégies de mot de passe de faible priorité sont appliquées après la stratégie en cours.

Gérer les stratégies de mot de passe

Les administrateurs disposant des droits appropriés peuvent gérer les stratégies de mot de masse à l'aide des tâches Afficher, Modifier, Créer et Supprimer une stratégie de mots de passe. Par défaut, ces tâches s'affichent dans la catégorie Stratégies.

Lorsque vous accédez à l'une de ces tâches, CA IdentityMinder affiche une liste de stratégies de mots de passe s'appliquant au magasin d'utilisateurs associé à l'environnement CA IdentityMinder actuel. Si CA IdentityMinder s'intègre à SiteMinder, la liste peut inclure des stratégies de mots de passe créées dans l'interface d'administration de SiteMinder à l'aide des services de mots de passe. Vous pouvez gérer les stratégies de mots de passe créées dans CA IdentityMinder ou SiteMinder.

Stratégies de mot de passe et base de données relationnelles

Si vous configurez une stratégie de mots de passe qui s'applique à une base de données relationnelle, vous devez utiliser le format suivant pour configurer l'attribut de données de mot de passe pour l'annuaire des utilisateurs SiteMinder :

tablename.columnname

Pour éviter les problèmes de syntaxe lors de l'exécution, nous recommandons que ce champ se trouve dans le tableau principal.

Critères de mot de passe d'intégration CA IdentityMinder et Siteminder

Lorsque CA IdentityMinder est intégré à SiteMinder et utilise les capacités de gestion des mots de passe de Siteminder, les stratégies de mot de passe sont obtenues à partir du magasin de stratégies de Siteminder. Dans ce cas, créez des mots de passe répondant aux critères de mot de passe de Siteminder. Les signes de ponctuation suivants sont les seuls à répondre aux critères de mot de passe de Siteminder :

'*', '(', '\',',','@','"',':','#','_','-','!','&','?',')','(','{','}','*','.','/'   "

Important : CA IdentityMinder n'impose aucune restriction quant à l'utilisation des signes de ponctuation dans les mots de passe. Toutefois, si vous comptez utiliser les capacités de mot de passe de Siteminder, nous vous recommandons de créer des mots de passe conformes aux restrictions de Siteminder.

Réinitialiser le mot de passe ou Déverrouiller un compte

Au cas où les utilisateurs oublieraient leurs mots de passe sur des systèmes Windows, vous pouvez configurer l'auto-administration de manière à afficher une invite sur l'écran d'ouverture de session Windows. Vous pouvez utiliser cette fonctionnalité en installant l'un de ces composants :

- Le composant GINA (Graphical Identification and Authorization, identification et autorisation graphiques) pour les systèmes Windows 2000, 2003, et XP
- Le Credential Provider pour les systèmes Windows VISTA et 2008

Cette fonctionnalité permet à l'utilisateur de se connecter à Self Service par l'intermédiaire du navigateur Web Cube si une page de requête de changement de mot de passe s'affiche. Une fois cette page remplie, l'utilisateur clique sur Revenir pour retourner sur l'écran d'ouverture de session Windows.

Installation de GINA ou du fournisseur d'informations d'identification

Vous pouvez installer GINA (pour les systèmes Windows 2000, 2003 et XP) ou le fournisseur d'informations d'identification (pour les systèmes Windows Vista et 2008) sur un système Windows depuis lequel un utilisateur accède à un environnement Identity Manager.

Pour installer GINA ou le fournisseur d'informations d'identification

1. Localisez le support de téléchargement ou d'installation des composants de provisionnement d'CA IdentityMinder.
2. Exécutez le programme d'installation sous l'agent.

   Remarque : Si vous installez le fournisseur d'informations d'identification sur un système d'exploitation 64 bits, choisissez la version 64 bits de ce logiciel.
3. Suivez les invites de l'assistant pour répondre aux questions.
4. Une fois le composant installé, configurez-le selon la procédure appropriée :
   - Configuration de GINA (page 118)
   - Configuration du fournisseur d'informations d'identification

Configuration de GINA

Vous pouvez utiliser l'outil de configuration GINA afin de modifier les valeurs GINA par défaut et les exporter dans un fichier de registre (.reg) pour un repackaging. Les paramètres peuvent aussi s'appliquer au système actuel.

Pour configurer GINA

1. Dans l'Explorateur Windows, accédez à l'emplacement d'installation de GINA. Exemple :

   ```
   C:\Program Files\CA\Identity Manager\Provisioning GINA
   ```

2. Double-cliquez sur l'exécutable suivant :

   ```
   ginaconfig.exe
   ```

3. Saisissez les informations dans les champs de paramètres de GINA.

   Link1 Command

   Ligne de commande complète à exécuter lorsqu'un utilisateur clique sur le lien Mot de passe oublié. Ce lien doit charger une URL vers une interface Web pour la réinitialisation du mot de passe. Par exemple, la commande peut être la suivante :

   ```
   http://eastern.local:8080/iam/im/pub/ca/index.jsp?task.tag=ForgottenPassw
   ord
   ```

   Pour cette URL, l'auto-inscription doit être activée dans l'environnement. De même, vérifiez que l'URL d'auto-administration pour l'environnement CA IdentityMinder est activée sur le système où vous installez GINA.

   Link2 Command

   Ligne de commande complète à exécuter lorsqu'un utilisateur clique sur le lien Déverrouiller un compte. Ce lien doit charger une URL vers une interface Web permettant à un utilisateur de déverrouiller un compte.

   Link3 Command

   Ligne de commande complète à exécuter lorsqu'un utilisateur clique sur le lien Nouveau compte. Ce lien doit charger une URL vers une interface Web permettant à un utilisateur de créer un compte.

   Utilisation d'une boîte de dialogue flottante

   Alternative aux commandes Lien, fournissant les mêmes fonctionnalités et s'affichant lors de la connexion à Windows. Cette boîte de dialogue peut également afficher une image BMP, WMF ou ICO à l'arrière-plan. Exemple de boîte de dialogue :

Domaine

Nom de domaine de provisionnement.

Conformité à la section 508 (utilisation de Revenir dans le menu)

Active la fonction Revenir dans un menu. Si cette case à cocher est désactivée, la boîte de dialogue Revenir est utilisée.

4. Remplissez les champs de paramètres de navigateur sécurisé comme suit.

   URL par défaut

   Page par défaut vers laquelle naviguer en l'absence de ligne de commande pour cmd_lien1 ou cmd_lien2.

   Liste d'autorisations

   Modèle d'expression régulière correspondant aux URL dont l'accès devrait toujours être autorisé.

   Liste d'interdictions

   Modèle d'expression régulière correspondant aux URL dont l'accès devrait toujours être interdit.

5. (Facultatif) Cliquez sur Exporter pour exporter vos paramètres vers un autre système.
6. Cliquez sur OK pour enregistrer vos paramètres.
7. Redémarrez le système.

Configurer le fournisseur d'informations d'identification

Vous pouvez utiliser un outil de configuration pour configurer le système sur lequel vous installez le fournisseur d'informations d'identification.

Pour configurer le fournisseur d'informations d'identification

1. Dans l'Explorateur Windows, accédez au répertoire d'installation du fournisseur d'informations d'identification. Exemple :

   C:\Program Files\CA\Identity Manager\Credential Provider

2. Double-cliquez sur l'exécutable suivant :

   CAIMCredProvConfig.exe

3. Remplissez les champs de paramètres du fournisseur d'informations d'identification de la manière suivante :

   Link1 URL

   Ligne de commande complète exécutée lorsqu'un utilisateur clique sur le lien Mot de passe oublié. Ce lien doit être une URL vers une interface Web pour la réinitialisation du mot de passe.

   Par exemple, la commande peut être la suivante :

   http://eastern.local:8080/iam/im/pub/ca/index.jsp?task.tag=ForgottenPasswor d

   Pour cette URL, l'auto-inscription doit être activée dans l'environnement. De même, vérifiez que l'URL d'auto-administration pour l'environnement CA IdentityMinder est activée sur le système où vous installez Credential Provider.

   Link2 **URL**

   Ligne de commande complète exécutée lorsqu'un utilisateur clique sur le lien Déverrouiller un compte. Ce lien doit être une URL vers une interface Web permettant à un utilisateur de déverrouiller un compte.

   Link3 URL

   Ligne de commande complète à exécuter lorsqu'un utilisateur clique sur le lien Nouveau compte. Ce lien doit correspondre à une URL vers une interface Web permettant à un utilisateur de créer un compte.

   Domaine

   Nom de domaine de provisionnement.

   Conformité à la section 508 (utilisation de Revenir dans le menu)

   Active la fonction Revenir dans un menu. Si cette case à cocher est désactivée, la boîte de dialogue Revenir est utilisée.

4. Remplissez les champs de paramètres de navigateur sécurisé comme suit.

   Liste d'autorisations

   Modèle d'expression régulière correspondant aux URL dont l'accès devrait toujours être autorisé.

   Liste d'interdictions

   Modèle d'expression régulière correspondant aux URL dont l'accès devrait toujours être interdit.

5. (Facultatif) Cliquez sur Exporter pour exporter vos paramètres vers un autre système.

6. Cliquez sur OK pour enregistrer vos paramètres.

7. Redémarrez le système.

Paramètres dans le registre

Quand vous disposez d'un outil de configuration pour définir GINA ou le Credential Provider, vous pouvez modifier le registre Windows afin de fournir les mêmes valeurs.

Paramètres du registre GINA

Si vous choisissez de ne pas utiliser l'outil de configuration de GINA, vous pouvez modifier les paramètres du registre Windows dans la clé suivante :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\GINAUNLOCK]
```

gina

Elle contient la valeur de l'option GINA chaînée actuelle. En général, il s'agira de MSGINA.DLL (Microsoft Windows GINA par défaut), à moins d'une intégration avec un produit comme Novell.

cmd_lien1

C'est la ligne de commande complète à exécuter pour le lien n°1 dans la boîte de dialogue de connexion.

cmd_lien2

C'est la ligne de commande complète à exécuter pour le lien facultatif n°2 dans la boîte de dialogue de connexion. Par exemple, vous pourriez ajouter un lien qui mènerait vers un site Web pour le déverrouillage de comptes.

Si la cmd_lien2 est vide, seule la cmd_ lien1 apparaît dans la fenêtre de la boîte de dialogue.

cmd_lien3

Il s'agit de la ligne de commande complète à exécuter lorsqu'un utilisateur clique sur le lien Nouveau compte. Ce lien doit charger une URL vers une interface Web permettant à un utilisateur de créer un compte.

comp508

Active la fonction Revenir dans un menu. Si cette case à cocher est désactivée, la boîte de dialogue Revenir est utilisée.

usecustomtitle

Affiche le titre personnalisé de l'outil GINA.

customtitle

Titre affiché dans l'outil GINA.

domaine

Nom de domaine de provisionnement.

langdir

L'emplacement des DLL de langue localisées.

configdir

Le chemin complet vers le répertoire d'installation de GINA.

rejectinvalidcerts

Contrôle si l'outil GINA accepte uniquement des certificats SSL valides. Si cette option est définie sur no, les certificats SSL expirés ou non valides sont autorisés.

Les valeurs valides pour cette clé sont *yes* et *no*.

Paramètres du registre du Credential Provider

Si vous choisissez de ne pas utiliser l'outil de configuration du Credential Provider, vous pouvez modifier les paramètres du registre Windows dans la clé suivante :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]
```

cmd_lien1

C'est la ligne de commande complète à exécuter pour le lien n°1 dans la boîte de dialogue de connexion. Ce lien doit correspondre à l'URL qui s'affiche lorsqu'un utilisateur clique sur le lien 1.

cmd_lien2

C'est la ligne de commande complète à exécuter pour le lien facultatif n°2 dans la boîte de dialogue de connexion. Ce lien doit correspondre à l'URL qui s'affiche lorsqu'un utilisateur clique sur le lien 2. Par exemple, vous pourriez ajouter un lien qui mènerait vers un site Web pour le déverrouillage de comptes.

Si la cmd_lien2 est vide, seule la cmd_ lien1 apparaît dans la fenêtre de la boîte de dialogue.

cmd_lien3

Il s'agit de la ligne de commande complète à exécuter lorsqu'un utilisateur clique sur le lien Nouveau compte. Ce lien doit charger une URL vers une interface Web permettant à un utilisateur de créer un compte.

usecustomtitle

Affiche le titre personnalisé pour Credential Provider.

customtitle

Titre affiché dans Credential Provider.

comp508

Active la fonction Revenir dans un menu. Si cette case à cocher est désactivée, la boîte de dialogue Revenir est utilisée.

domaine

Nom de domaine de provisionnement.

langdir

L'emplacement des DLL de langue localisées.

disablepwdcp

L'option Désactiver Microsoft Password Credential Provider. 1 est désactivé. 0 est activé.

CredentialProviderInstallPath

Le chemin complet vers le répertoire d'installation du Credential Provider.

configdir

Le chemin complet vers le répertoire d'installation du Credential Provider.

rejectinvalidcerts

Contrôle si Credential Provider accepte uniquement les certificats SSL valides. Si cette option est définie sur no, les certificats SSL expirés ou non valides sont autorisés.

Les valeurs valides pour cette clé sont *yes* et *no*.

Paramètres du registre du navigateur Cube

Les composants du navigateur sécurisé Cube ont plusieurs valeurs de registre qui contrôlent leur comportement. Les valeurs de Cube se trouvent dans la clé de registre suivante :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Cube]
```

404

Le chemin vers un document HTML standard à afficher si la machine ne peut pas contacter le serveur de provisionnement à distance au démarrage.

par défaut

La page par défaut vers laquelle naviguer quand aucune URL n'est comprise dans la Commande de Lien1 ou la Commande de Lien2.

autorisé

ACL autorisées explicites. Un modèle d'expression régulière correspondant aux URL qui sont toujours autorisées. Pour plus d'informations, reportez-vous aux listes de contrôle d'accès de Cube (page 127).

interdire

ACL interdites explicites. Un modèle d'expression régulière correspondant aux URL dont l'accès devrait toujours être interdit. Pour plus d'informations, reportez-vous aux listes de contrôle d'accès de Cube (page 127).

langdir

L'emplacement des DLL de langue localisées.

Listes de contrôle d'accès de Cube

Les ACL de Cube sont des modèles d'expression régulières qui autorisent ou interdisent explicitement de naviguer vers une URL sélectionnée. ACL effectue selon l'ordre suivant :

1. Autoriser (la permission est automatiquement accordée d'abord)
2. Interdire (les URL interdites sont vérifiées ensuite)

Exemples de liste de contrôle d'accès de GINA

"autoriser"="(.pdf)"

Autoriser l'affichage de tous les documents PDF.

"interdire"="(.doc|.xls)"

Interdire l'accès aux documents Microsoft Word et Excel.

Personnalisation du message Alimenté par

Un message "Alimenté par..." s'affichera peut-être dans la boîte de dialogue Renvoyer ou dans l'option de menu Renvoyer de l'outil GINA ou de Credential Provider. Vous pouvez modifier ou supprimer ce message.

Pour personnaliser le message Alimenté par

1. Téléchargez ResEdit, un éditeur de ressources gratuit disponible à l'adresse http://www.resedit.net.
2. Démarrez ResEdit.
3. Modifiez le fichier 1033.dll dans le dossier des langues.
4. Double-cliquez sur Table de chaînes.
5. Supprimez ou modifiez l'ID de ressource 135, la version anglaise de la ressource de ce message.

Réinitialisation d'un mot de passe pour une connexion Windows

Une fois que GINA ou le Credential est installé sur un système Windows, un lien Mot de passe oublié apparaît dans la boîte de dialogue d'ouverture de session Microsoft Windows standard. Ce lien permet de réinitialiser votre mot de passe ou de voir des indices qui vous aident à vous en souvenir.

Pour réinitialiser un mot de passe de connexion Windows

1. Cliquez sur Connexion dans la boîte de dialogue de sécurité de Windows. La boîte de dialogue Connexion de Windows s'affiche.
2. Entrez un nom d'utilisateur valide.
3. Cliquez sur Mot de passe oublié.

   .La page d'indice de mot de passe d'CA IdentityMinder s'affiche.

   Si vous vous souvenez de votre mot de passe, retournez à la boîte de dialogue de connexion pour continuer. Sinon, passez à l'étape 4 pour vous authentifier dans CA IdentityMinder Self Service.
4. Tapez les réponses aux questions d'authentification.

   Remarque : Si vous ne connaissez pas la réponse à toutes les questions, cliquez sur Requête pour demander que votre mot de passe soit réinitialisé par un administrateur.
5. Si vous réussissez à répondre aux questions, cliquez sur Connexion.

   Le système vous connecte et ouvre Self Service.
6. Modification du mot de passe
7. Retournez à la boîte de dialogue de connexion et connectez-vous avec le nouveau mot de passe.

Installation silencieuse de GINA

GINA prend en charge un mode d'installation silencieux. Six propriétés sont prises en charge.

LINK1

Fait référence au chemin SOFTWARE\ComputerAssociates\GINAUNLOCK\link1_cmd dans le registre.

LINK2

Fait référence au chemin SOFTWARE\ComputerAssociates\GINAUNLOCK\link2_cmd dans le registre.

LINK3

Fait référence au chemin SOFTWARE\ComputerAssociates\GINAUNLOCK\link3_cmd dans le registre.

GNADOMAIN

Fait référence au chemin SOFTWARE\ComputerAssociates\GINAUNLOCK\domain dans le registre.

COMP508

Fait référence au chemin SOFTWARE\ComputerAssociates\GINAUNLOCK\comp508 dans le registre.

USECUSTOMTITLE

Fait référence au chemin SOFTWARE\ComputerAssociates\Cube\usecustomtitle dans le registre.

CUSTOMTITLE

Fait référence au chemin SOFTWARE\ComputerAssociates\Cube\customtitle dans le registre.

REJECTINVALIDCERTS

Fait référence au chemin SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts dans le registre.

UNREACHABLE

Fait référence à l'emplacement de la page non accessible.

La syntaxe permettant de définir la valeur de ces propriétés se présente comme suit :

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program
Files\CA\Identity Manager\Provisioning GINA\"
LINK1=\"[INSTALLDIR]cube <url>\" LINK2=\"[INSTALLDIR]cube <url>\"
LINK3=\"[INSTALLDIR]cube <url>\"  COMP508=\"yes\"
REJECTINVALIDCERTS=\"yes\" USECUSTOMTITLE=\"yes\"
CUSTOMTITLE=\"custom gina title\""
```

ou

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program
Files\CA\Identity Manager\Provisioning GINA\"
LINK1=\"[INSTALLDIR]cube <url>\" LINK2=\"[INSTALLDIR]cube <url>\"
LINK3=\"[INSTALLDIR]cube <url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom gina title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"<url>\""
```

ou

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program
Files\CA\Identity Manager\Provisioning GINA\"
LINK1=\"[INSTALLDIR]cube <url>\" LINK2=\"[INSTALLDIR]cube <url>\"
LINK3=\"[INSTALLDIR]cube <url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom gina title\"
SELECTDEFAULTCREDENTIAL=\"yes\"
UNREACHABLE=\"file:///[INSTALLDIR]<file name>\""
```

[INSTALLDIR]

Fait référence à la valeur de la propriété INSTALLDIR.

<url>

Spécifie l'URL pour un compte déverrouillé ou un mot de passe oublié.

<file name>

Définit le nom du fichier inaccessible.

Installation silencieuse de Credential Provider

L'outil Credential Provider prend en charge un mode d'installation silencieux. Six propriétés sont prises en charge.

LINK1

Fait référence au chemin SOFTWARE\CA\CAIMCredentialProvider\link1_cmd dans le registre.

LINK2

Fait référence au chemin SOFTWARE\CA\CAIMCredentialProvider\link2_cmd dans le registre.

LINK3

Fait référence au chemin SOFTWARE\CA\CAIMCredentialProvider\link3_cmd dans le registre.

DOMAIN

Fait référence au chemin SOFTWARE\CA\CAIMCredentialProvider\domain dans le registre.

COMP508

Fait référence au chemin SOFTWARE\CA\CAIMCredentialProvider\comp508 dans le registre.

USECUSTOMTITLE

Fait référence au chemin SOFTWARE\CA\Cube\usecustomtitle dans le registre.

CUSTOMTITLE

fait référence au chemin SOFTWARE\CA\Cube\customtitle dans le registre.

REJECTINVALIDCERTS

fait référence au chemin SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts dans le registre.

UNREACHABLE

Fait référence à l'emplacement de la page non accessible.

La syntaxe permettant de définir la valeur de ces propriétés se présente comme suit :

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\"LINK3=\"<url>\"
COMP508=\"yes\" REJECTINVALIDCERTS=\"yes\" USECUSTOMTITLE=\"yes\"
CUSTOMTITLE=\"custom cp title\""
```

ou

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\" LINK3=\"<url>\"
COMP508=\"yes\" USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"<url>\""
```

ou

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\"
LINK1=\"<url>\" LINK2=\" <url>\" LINK3=\"<url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"file:///[INSTALLDIR]<file name>\""
"Yes\""
```

[INSTALLDIR]

Fait référence à la valeur de la propriété INSTALLDIR.

<url>

Spécifie l'URL pour un compte déverrouillé ou un mot de passe oublié.

<file name>

Définit le nom du fichier inaccessible.

Chapitre 6: Synchronisation des mots de passe sur des terminaux

Vous pouvez installer un agent de synchronisation du mot de passe sur certains terminaux pris en charge par CA IdentityMinder. L'agent intercepte les demandes de changement de mot de passe sur le terminal et soumet les modifications au serveur de provisionnement.

Ce chapitre traite des sujets suivants :

Mots de passe sous Windows

CA IdentityMinder peut intercepter la modification du mot de passe d'un compte Windows natif et propager le nouveau mot de passe vers un utilisateur et tous les comptes lui appartenant.

Lorsque l'agent de synchronisation du mot de passe détecte une tentative de modification de mot de passe, il intercepte la demande et l'envoie au serveur de provisionnement. Le serveur de provisionnement propage alors le nouveau mot de passe à l'utilisateur et à ses autres comptes associés.

La configuration requise de la synchronisation du mot de passe se présente comme suit :

- L'agent de synchronisation du mot de passe doit être installé sur le système sur lequel la modification du mot de passe doit être interceptée.
- Le système doit être géré comme un terminal acquis.
- La case à cocher Agent de synchronisation du mot de passe installé doit être activée dans l'onglet Paramètres du terminal acquis.
- Les comptes sur les systèmes gérés doivent être explorés et corrélés avec les utilisateurs CA IdentityMinder.
- L'environnement doit autoriser la provenance des modifications de mot de passe à partir des comptes de terminal. Un administrateur disposant d'un accès à la console de gestion active cette fonctionnalité.

Important : Veillez à formuler les règles de mot de passe avec soin, de sorte qu'un seul mot de passe s'applique à tous les systèmes. Par exemple, si les mots de passe Windows doivent comporter douze caractères, les systèmes qui acceptent les mots de passe de dix caractères au maximum rejettent la modification lors de la synchronisation.

Le serveur CA IdentityMinder ne tient pas compte des restrictions de mot de passe sur le terminal. Dans le cadre de l'utilisation des comptes de terminaux, la stratégie de mot de passe doit être plus stricte que celle appliquée sur les terminaux.

Installation de l'agent de synchronisation du mot de passe

Vous pouvez installer l'agent de synchronisation du mot de passe sur les ordinateurs Windows gérés auxquels des utilisateurs globaux se connectent. L'agent s'exécute en arrière-plan sur ces ordinateurs.

Exécution du script d'installation

Tenez compte des conditions requises suivantes :

- Le serveur de provisionnement doit gérer le système sur lequel vous installez l'agent.
- Créez un utilisateur qui agira en tant qu'administrateur des modifications de mot de passe. Il est recommandé d'utiliser le nom etapwsad. Le profil de cet utilisateur doit être PasswordAdministrator.
- Deux agents de synchronisation de mot de passe Windows existent dans le média d'installation : l'un pour Windows 32 bits et l'autre pour 64 bits. L'agent de synchronisation du mot de passe 32 bits n'est pas pris en charge sous Windows 64 bits. La norme FIPS est uniquement prise en charge par l'agent de synchronisation du mot de passe 32 bits.

Procédez comme suit:

1. Recherchez le média d'installation CA IdentityMinder.
2. Accédez à \Agent\PasswordSync ou à \Agent\PasswordSync-x64.
3. Exécutez setup.exe.
4. Répondez à l'assistant de configuration comme suit :
   a. Dans le champ Nom d'hôte, indiquez le nom du système du serveur de provisionnement.

b. Si l'installation de votre serveur de provisionnement utilise un port autre qu'un port par défaut, appliquez les modifications nécessaires.

   Le port LDAP recommandé et utilisé pour la connexion au serveur de provisionnement est 20390.

c. Pour récupérer le domaine du serveur de provisionnement, cliquez sur Find domain (Rechercher le domaine).

d. Si l'installation de votre serveur de provisionnement est configurée pour le basculement, suivez les instructions à l'écran pour ajouter une liste de serveurs séparée par des virgules.

e. Cliquez sur Suivant.

f. Dans le champ Administrateur, entrez etapwsad comme nom d'utilisateur global par défaut pour l'agent de synchronisation du mot de passe. Le profil de cet utilisateur doit être PasswordAdministrator. qui n'existe pas par défaut.

g. Dans le champ Administrateur de mots de passe, entrez le mot de passe de l'administrateur.

h. Cliquez sur Suivant.

i. Dans la liste déroulante Type de terminal, sélectionnez le type de terminal de l'hôte sur lequel vous installez l'agent.

j. Dans la liste déroulante Nom du terminal, sélectionnez le nom utilisé lors de la création du terminal dans la console d'utilisateur.

k. Cliquez sur Configurer.

5. Lorsque vous êtes invité à terminer l'installation, cliquez sur Terminer et redémarrez.

Mise à jour du terminal dans la console d'utilisateur

Dans la console d'utilisateur, mettez à jour le terminal pour indiquer que l'agent est installé.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur.
2. Cliquez sur Terminaux, Gérer les terminaux, Modifiez le terminal.
3. Recherchez le terminal sur lequel l'agent est installé.
4. Cliquez sur l'onglet Paramètres du terminal.
5. Sélectionnez la case à cocher Agent de synchronisation du mot de passe installé.

Activation d'un environnement pour la synchronisation de mot de passe

Après avoir installé l'agent de synchronisation du mot de passe, vous devez autoriser l'environnement à recevoir les modifications de mot de passe appliquées aux terminaux. Pour cette tâche, un administrateur requiert l'accès à la console de gestion et à CA Directory pour permettre à l'environnement d'accepter ces modifications.

Procédez comme suit:

1. Pour les nouveaux utilisateurs, utilisez la console de gestion comme suit :
   a. Sélectionnez l'environnement.
   b. Cliquez sur Advanced Settings (Paramètres avancés), Provisonning (Provisionnement).
   c. Sélectionnez la case à cocher Enable Password Changes (Activer les modifications de mot de passe) sous Endpoint Accounts (Comptes de de terminal).
2. Pour les utilisateurs existants, définissez l'attribut eTPropagatePassword sur 1 dans CA Directory.

Configuration de serveurs secondaires pour l'agent de synchronisation du mot de passe

Pour configurer un serveur secondaire pour l'agent de synchronisation du mot de passe, utilisez l'assistant Configuration de l'agent de synchronisation du mot de passe.

Pour ajouter un serveur secondaire pour l'agent de synchronisation du mot de passe :

1. Exécutez PwdSyncConfig.exe, situé dans le répertoire *dossier_de_synchronisation_de_mot_passe*\bin.
2. Entrez les informations de configuration suivantes.

   Hôte

   Spécifiez le nom d'hôte du serveur de provisionnement principal.

   Cette action permet de renseigner le champ URL du serveur avec le nom d'hôte spécifié.

   Port LDAP

   Spécifiez le numéro de port que l'ordinateur utilise pour se connecter au serveur de provisionnement.

   CA IdentityMinder renseigne le champ URL du serveur avec l'hôte et le port spécifiés.
3. Pour obtenir la liste des domaines, cliquez sur Rechercher le domaine.
4. Dans la zone déroulante Domaine, sélectionnez le nom du domaine, puis cliquez sur Suivant.

5. Ajoutez le nom d'hôte et le port des serveurs secondaires dans le champ URL du serveur au format suivant.

   ldaps://*hôte_principal*:20390,ldaps://*hôte_secondaire*:20390

6. Cliquez sur Suivant.
7. Renseignez les champs restants dans l'assistant de configuration.

Fonctionnement de l'agent de synchronisation du mot de passe

Le processus de propagation commence lorsque les utilisateurs globaux modifient leurs mots de passe sur un système Windows. Une fois le mot de passe saisi, les événements suivants se produisent.

1. Le système d'exploitation Windows vérifie que le mot de passe est conforme à la stratégie de mot de passe définie. Si Windows refuse le mot de passe, la demande de modification est rejetée, un message d'erreur s'affiche et aucune autre action n'est entreprise (y compris la synchronisation).
2. Le système Windows transmet la demande de modification du mot de passe à l'agent de synchronisation du mot de passe CA IdentityMinder, qui l'envoie éventuellement au serveur de provisionnement à des fins de contrôle de qualité du mot de passe. Si le mot de passe ne respecte pas les règles de qualité d'CA IdentityMinder, la demande de modification est rejetée et un message d'erreur s'affiche. Le mot de passe Windows reste inchangé et aucune synchronisation n'est effectuée.
3. L'agent de synchronisation du mot de passe envoie un mot de passe conforme aux règles de qualité de Windows et d'CA IdentityMinder au serveur de provisionnement en vue de sa propagation.
4. CA IdentityMinder met à jour le mot de passe d'utilisateur global et propage le nouveau mot de passe vers une partie ou l'ensemble des comptes associés à l'utilisateur global.

Remarque : Vos stratégies de mot de passe pour Windows et CA IdentityMinder doivent être identiques ou cohérentes. En effet, les messages d'erreur s'affichent en fonction de la stratégie de mot de passe de Windows, même si CA IdentityMinder rejette la demande.

Le paramètre de configuration password_update_timeout (eta_pwdsync.conf) spécifie le délai (en secondes) pendant lequel l'agent de synchronisation du mot de passe attend la confirmation de propagation de la modification du mot de passe reçue du serveur CA IdentityMinder. Si l'agent de synchronisation du mot de passe ne reçoit pas de confirmation avant l'expiration du délai, il agit comme si la propagation s'était correctement déroulée et consigne un avertissement (eta_pwdsync.log) indiquant l'impossibilité de vérifier la propagation du mot de passe modifié. La valeur minimum de ce paramètre, zéro (0), indique que l'agent de synchronisation du mot de passe n'attend pas la confirmation. Pour plus d'informations, reportez-vous à la rubrique eta_pwdsync.conf--Configuration de l'agent de synchronisation du mot de passe dans l'aide du gestionnaire de provisionnement.

Contrôle de qualité de mot de passe au niveau compte

Le contrôle de qualité de mot de passe est effectué lorsque des comptes sur les terminaux gérés sont créés ou modifiés, ou lorsqu'un mot de passe d'utilisateur global est défini. Le contrôle de qualité de mot de passe se limite aux vérifications basées sur les caractères du mot de passe. Les vérifications appliquées aux utilisateurs globaux basées sur l'historique des modifications récentes (fréquence de mise à jour du mot de passe et fréquence de réutilisation du mot de passe) ne sont pas effectuées sur les comptes, car CA IdentityMinder n'intercepte pas toutes les modifications des mots de passe de compte. Par conséquent, il ne dispose pas d'un historique précis des modifications de mot de passe avec lequel effectuer ces vérifications.

La vérification des mots de passe de compte est contrôlée par les paramètres de configuration de domaine suivants.

- Type de terminal/Contrôler les mots de passe de compte
- Type de terminal/Contrôler les mots de passe de compte vides

Les valeurs des paramètres spécifient le niveau de vérification à effectuer pour chaque terminal géré. Le terminal peut être spécifié comme suit.

```
ALL
-ALL
<Nom_espace_de_noms>
-<Nom_espace_de_noms>
<Nom_espace_de_noms>:<Nom_répertoire>
-<Nom_espace_de_noms>:<Nom_répertoire>
```

Les formes incluant le signe moins (-) désactivent le paramètre, contrairement aux formes sans ce signe qui activent le paramètre. Les formes [-]<Nom_espace_de_noms> contrôlent tous les terminaux du type de terminal indiqué, tandis que les formes [-]<Nom_espace_de_noms>:<Nom_répertoire> contrôlent les terminaux individuels. Les formes [-]ALL contrôlent tous les terminaux, quel que soit leur type. La valeur par défaut des deux paramètres est -ALL.

Chaque paramètre peut être spécifié plusieurs fois. Si plusieurs valeurs spécifient le même terminal, la dernière valeur est utilisée. Vous pouvez placer les règles générales en premier, puis les règles spécifiques destinées à remplacer la règle générale.

Le paramètre Contrôler les mots de passe de compte effectue des vérifications équivalentes à celle du contrôle de qualité de mot de passe de l'utilisateur global. Lorsque ce paramètre est activé pour un terminal, CA IdentityMinder vérifie les mots de passe inclus dans une demande de modification pour un compte existant, y compris les tentatives de définition d'un mot de passe vide. Lors de la création d'un compte, le contrôle de qualité de mot de passe n'est pas effectué si aucun mot de passe n'est fourni.

Le paramètre Contrôler les mots de passe de compte vides permet de contrôler les mots de passe vides lors de la création des comptes. Si le profil de mot de passe est activé et requiert au moins un mot de passe à un caractère, un mot de passe vide provoque l'échec de la création du compte. Ce paramètre est distinct du paramètre Contrôler les mots de passe de compte, car dans certains types de terminaux, il est acceptable de créer un compte sans mot de passe.

Remarque : Le contrôle de qualité de mot de passe est ignoré pour les mots de passe de compte synchronisés si le mot de passe fourni correspond au mot de passe actuel de l'utilisateur global.

Application de la qualité de mot de passe

L'option de synchronisation de mots de passe intercepte les demandes de modification de mot de passe sur les systèmes natifs (par exemple, Windows NT/ADS) et les soumet au serveur CA IdentityMinder. Le serveur synchronise le mot de passe de l'utilisateur global et les mots de passe de compte associés à l'utilisateur global. Les règles de qualité de mot de passe d'CA IdentityMinder pour un profil de mot de passe et du système natif (Windows NT/ADS) permettent d'appliquer le contrôle de qualité de mot de passe.

Configuration de la synchronisation de mots de passe

Initialement, l'agent de synchronisation du mot de passe est configuré lors de l'installation, mais il peut être reconfiguré à tout moment à l'aide de l'assistant de configuration de synchronisation du mot de passe. Il est possible d'effectuer d'autres configurations. Par exemple, vous pouvez changer des paramètres de la vérification de la qualité de mot de passe ou les délais d'expiration, à l'aide du fichier eta_pwdsync.conf.

Ce fichier se trouve dans le dossier password_sync_folder\data\. Dans ce fichier de configuration, toutes les clés sont définies lors de l'installation de l'agent de synchronisation du mot de passe. Par conséquent, changez ces clés uniquement si cela est nécessaire. Pour plus d'informations, consultez le texte de ce fichier.

Important : Par mesure de précaution, créez une sauvegarde du fichier de configuration avant de le modifier.

Section [Server]

Clé	Description	Par défaut
hôte	Spécifie le serveur de domaine qui gère la propagation du mot de passe.	Aucun
port	Spécifie le port d'écoute LDAP du serveur de provisionnement.	20411

Clé	Description	Par défaut
use_tls	Spécifie si TLS/SSL est utilisé pour sécuriser la communication entre l'agent de synchronisation du mot de passe et le serveur de provisionnement.	Oui
admin_suffix	Spécifie le suffixe du domaine de l'administrateur que l'agent de synchronisation du mot de passe utilise pour se connecter à CA IdentityMinder.	Aucun
admin	Spécifie le nom du compte de l'administrateur que l'agent de synchronisation du mot de passe utilise pour se connecter à CA IdentityMinder.	Aucun
password	Spécifie le mot de passe du nom du compte spécifié dans la clé d'administrateur.	Aucun

Section [eTaDomain]

Clé	Description	Par défaut
Domaine	Spécifie le domaine de provisionnement dans lequel vous avez installé l'agent de synchronisation du mot de passe.	Aucun
etrust_suffix	Spécifie le suffixe du produit CA IdentityMinder complet.	Aucun
domain_suffix	Spécifie le suffixe du domaine de provisionnement.	Aucun
type de terminal	Spécifie le type de terminal sur lequel vous avez installé l'agent de synchronisation du mot de passe.	Aucun
endpoint	Spécifie le terminal pour lequel l'agent de synchronisation du mot de passe intercepte les mots de passe.	Aucun
endpoint_dn	Spécifie le nom unique du terminal.	Aucun
container_dn	Spécifie le nom unique du conteneur qui contient les comptes dont les mots de passe sont en cours de modification.	Aucun
acct_attribute_name	Spécifie le nom d'attribut du compte, par exemple : eTN16AccountName pour Windows NT.	Il varie en fonction du type de terminal.

Clé	Description	Par défaut
acct_object_class	Spécifie l'objectClass des comptes.	Il varie en fonction du type de terminal.

Section [PasswordProfile]

Clé	Description	Par défaut
profile_enabled	Spécifie si la fonctionnalité de vérification du profil de mot de passe est activée.	Non
profile_dn	Spécifie si l'assistant de configuration de mot de passe génère un nom unique pour le profil de mot de passe.	eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

Section [Timeout]

Clé	Description	Par défaut
search_acct_dn	Spécifie la valeur du délai d'expiration lors de la recherche du nom unique du compte.	120 secondes
pwd_update	Spécifie la valeur du délai d'expiration lors de la propagation des mots de passe.	400 secondes
pwd_quality_check	Spécifie la valeur du délai d'expiration (en secondes) lors de la vérification de la qualité des mots de passe.	1

Section [Logs]

Clé	Description	Par défaut
log_file	Spécifie le fichier journal qui contient les messages journalisés à partir de l'agent de synchronisation du mot de passe.	..\Program files\CA\Identity Manager Password Sync Agent
log_level	Spécifie le niveau de journalisation. Valeurs valides : 1 : fichier d'initialisation 2 : réussite ou échec de la mise à jour du mot de passe 3 : débogage de la connexion 4 : suivi	0 : aucune journalisation

Basculement

Si le serveur de provisionnement est hors service ou très chargé, l'agent de synchronisation du mot de passe peut basculer vers un autre serveur. Le basculement requiert que plusieurs serveurs de provisionnement interviennent sur le même domaine et que l'agent les utilise.

La section de configuration de l'agent pour l'utilisation de serveurs auxiliaires (page 136) contient des instructions de configuration.

Activation des messages de journal

Pour connaître la raison du rejet de la modification d'un mot de passe, consultez les messages de journal reçus de l'agent de synchronisation du mot de passe. Les messages journalisés sont stockés dans le fichier eta_pwdsync.log. Par défaut, celui-ci est situé dans le dossier \Program files\CA\Agent de synchronisation du mot de passe CA IdentityMinder.

La journalisation de l'agent de synchronisation du mot de passe (incluse dans le fichier eta_pwdsync.log) contient les messages ci-dessous.

- Messages d'erreur (journalisés systématiquement)
- Messages de diagnostic (flux de processus, trace) que vous pouvez activer ou désactiver à l'aide du paramètre logging_enabled=yes|no du fichier eta_pwdsync.conf

Pour optimiser le diagnostic des problèmes, consultez le fichier eta_pwdsync.log et le journal du serveur de provisionnement (en vous référant à une même période).

Bien qu'obsolète, l'ancien paramètre de configuration log_level a été conservé à des fins de compatibilité descendante : log_level=0 a été remplacé par logging_enabled=no et log_level=anything else par logging_enabled=yes. Si le fichier de configuration inclut de nouveaux paramètres et des paramètres anciens, le paramètre explicite logging_enabled=yes|no remplace le paramètre indirect exécuté par l'ancien paramètre log_level=number.

Remarque : L'agent n'inclut plus la liste des connecteurs disponibles qui figurait auparavant dans le fichier eta_pwdsync.log.

Vérification de l'installation

Une fois l'agent de synchronisation du mot de passe installé, modifiez un mot de passe sur le système Windows pour vérifier que le mot de passe d'utilisateur global associé au compte est également modifié.

Mots de passe sous UNIX et Linux

CA IdentityMinder peut intercepter la modification du mot de passe d'un compte dans un système UNIX ou Linux et la propager à tous les autres comptes associés à son utilisateur global. Le composant utilisé pour l'authentification des mots de passe sur des systèmes de sécurité externes est appelé module d'authentification enfichable (PAM). Avec PAM, CA IdentityMinder authentifie les mots de passe sur des systèmes de sécurité externes de sorte que les utilisateurs globaux puissent utiliser leur mot de passe de système existant pour se connecter à CA IdentityMinder.

Synchronisation de mots de passe UNIX

Un module de synchronisation de mots de passe est fourni et détecte des événements de modification de mot de passe dans la structure PAM UNIX. Le module de synchronisation de mots de passe UNIX notifie le serveur de provisionnement d'une modification de mot de passe. Le serveur de provisionnement recherche l'utilisateur global associé et propage les modifications vers d'autres comptes liés automatiquement.

Les systèmes d'exploitation UNIX qui prennent en charge la structure PAM incluent les éléments suivants :

- AIX v5.3 sur la plate-forme Power avec PAM activé
- HP-UX v11.00 sur une plate-forme PA-RISC et plates-formes Itanium® 2
- Solaris v2.6 et versions ultérieures sur les plates-formes Sparc et Intel
- Linux 32 bits avec glibc v2.2 et versions ultérieures sur la plate-forme s390 ou Intel i386

  Remarque : Pour les plates-formes Linux, le fichier binaire test_sync doit être accessible à tous les utilisateurs, mais seuls l'utilisateur root, le propriétaire, doivent disposer d'autorisation d'exécution.

  Pour ajouter cette bibliothèque à l'emplacement accessible pour tous les utilisateurs, incluez cette commande dans le fichier /etc/bashrc global :

  ```
  export PATH=$PATH:/etc/pam_CA_eta
  ```

Fonctionnement d'UNIX PAM

Le processus suivant décrit les fonctions de la fonctionnalité UNIX PAM :

1. Le mot de passe d'un utilisateur UNIX doit être modifié pour l'une des raisons suivantes :
   - Décision de l'utilisateur
   - L'utilisateur est obligé de changer le mot de passe à l'aide des paramètres système ou manuellement.
   - Le mot de passe de l'utilisateur est modifié par un administrateur.
2. Le nouveau mot de passe est soumis au service de mots de passe de la structure PAM.
3. Le service de mots de passe de la structure PAM appelle la bibliothèque PAM pour mettre à jour les fichiers de sécurité UNIX locaux.
4. Le service de mots de passe de la structure PAM appelle le module de synchronisation de mot de passe UNIX (pam_CA_eta) pour notifier le serveur de provisionnement de la modification du mot de passe.
5. Le serveur de provisionnement met à jour le mot de passe de l'utilisateur global associé et de tous ses comptes associés.

Configuration requise pour l'utilisation de la synchronisation de mot de passe UNIX

La configuration requise pour l'utilisation de la fonctionnalité de synchronisation de mots de passe UNIX se présente comme suit :

- L'agent de synchronisation de mot de passe UNIX doit être installé sur le système UNIX sur lequel vous voulez détecter les modifications de mot de passe.
- L'agent distant UNIX et CAM doivent être installés sur le système UNIX sur lequel l'agent de synchronisation de mot de passe UNIX réside.
- Le système doit être géré comme un terminal acquis. La case à cocher Agent de synchronisation du mot de passe installé doit être activée dans les propriétés du terminal acquis.
- Les comptes sur les systèmes gérés doivent être explorés et corrélés avec les utilisateurs globaux.
- L'environnement doit autoriser la provenance des modifications de mot de passe à partir des comptes de terminal. Un administrateur disposant d'un accès à la console de gestion active cette fonctionnalité.

Installation de la fonctionnalité UNIX PAM

Pour installer UNIX PAM, procédez comme suit.

Pour installer la fonctionnalité UNIX PAM :

1. Sélectionnez le fichier de package qui correspond à votre plate-forme UNIX :

Système d'exploitation UNIX	Nom du fichier de package
HP-UX v11 PA-RISC	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX Itanium2	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 Power	pam_CA_eta-1.1.AIX.tar.Z
Solaris Sparc	pam_CA_eta-1.1.Solaris.tar.Z
Solaris Intel	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux x86	pam_CA_eta-1.1.Linux.tar.gz
Linux s390	pam_CA_eta-1.1.LinuxS390.tar.gz

2. Transférez le fichier de package de votre choix vers un dossier temporaire (/tmp) sur le serveur UNIX à l'aide de FTP en mode binaire, ou d'un autre outil de transfert de fichiers prenant en charge les fichiers binaires. Un exemple de session de transfert peut s'afficher comme suit :

```
W:\Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01.company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1,1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1,1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```

3. Connectez-vous en tant qu'utilisateur root sur le serveur UNIX et extrayez le fichier de package :

```
# cd /tmp
# zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
```

   Sous Linux, utilisez la commande suivante :

```
# tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
```

4. Copiez les fichiers de configuration et TLS dans le dossier de configuration par défaut :

```
# cd pam_CA_eta-1.1
# mv pam_CA_eta /etc
```

5. Copiez le module pam_CA_eta dans le dossier de bibliothèques de sécurité :

   Sous AIX, utilisez la commande suivante :

```
# cp -p pam_CA_eta.o /usr/lib/security/
```

   Sous HP-UX, utilisez la commande suivante :

```
# cp -p libpam_CA_eta.1 /usr/lib/security/
```

   Sous HP-UX Itanium2, utilisez la commande suivante :

```
# cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
```

   Sous Linux i386 ou s390, utilisez la commande suivante :

```
# cp -p pam_CA_eta.so /lib/security/
```

   Sous Solaris Sparc ou Intel, utilisez la commande suivante :

```
# cp -p pam_CA_eta.so /usr/lib/security/
```

6. (Facultatif) Copiez les programmes d'évaluation :

```
# cp -p test_* /etc/pam_CA_eta
# cp -p pam_test* (/usr)/lib/security/
```

Informations complémentaires

Dépannage de la synchronisation de mot de passe UNIX (page 154)

Mise à jour du terminal dans la console d'utilisateur

Dans la console d'utilisateur, mettez à jour le terminal pour indiquer que l'agent est installé.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur.
2. Cliquez sur Terminaux, Gérer les terminaux, Modifiez le terminal.
3. Recherchez le terminal sur lequel l'agent est installé.
4. Cliquez sur l'onglet Paramètres du terminal.
5. Sélectionnez la case à cocher Agent de synchronisation du mot de passe installé.

Activation d'un environnement pour la synchronisation de mot de passe

Après avoir installé l'agent de synchronisation du mot de passe, vous devez autoriser l'environnement à recevoir les modifications de mot de passe appliquées aux terminaux. Pour cette tâche, un administrateur requiert l'accès à la console de gestion et à CA Directory pour permettre à l'environnement d'accepter ces modifications.

Procédez comme suit:

1. Pour les nouveaux utilisateurs, utilisez la console de gestion comme suit :
    a. Sélectionnez l'environnement.
    b. Cliquez sur Advanced Settings (Paramètres avancés), Provisonning (Provisionnement).
    c. Sélectionnez la case à cocher Enable Password Changes (Activer les modifications de mot de passe) sous Endpoint Accounts (Comptes de de terminal).
2. Pour les utilisateurs existants, définissez l'attribut eTPropagatePassword sur 1 dans CA Directory.

Configuration de la fonctionnalité de synchronisation de mot de passe UNIX

La configuration de la fonctionnalité de synchronisation de mot de passe UNIX implique la définition des paramètres dans les fichiers suivants :

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

Important : Le mot de passe d'un utilisateur disposant de droits élevés étant stocké dans le fichier de configuration pam_CA_eta.conf, ce fichier doit être uniquement lisible par le compte racine. Notez que les paramètres dans le fichier de package incluent owner=root et mode=500 et que le commutateur -p de la commande cp les préserve lors de l'installation.

Configuration du fichier pam_CA_eta.conf

Pour configurer le fichier pam_CA_eta.conf, procédez comme suit.

Pour configurer le fichier pam_CA_eta.conf :

1. Accédez au dossier /etc/pam_CA_eta.
2. Modifiez le fichier pam_CA_eta.conf. Ce fichier de configuration contient sa propre documentation.

```
#
#   CA - CA IdentityMinder
#
#   pam_CA_eta.conf
#
#   Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA IdentityMinder LDAP server primary and optional alternate
server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA IdentityMinder LDAP server
# value: a valid TCP/IP port number
# default: 20390
# port 20390


# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#              server is used.
#              Cloud based server is accessed by proxying the requests
#              through the on-premise CS, requiring use of remote-server
#              set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA IdentityMinder
server
# value: a numeric value
# default: 100
# size-limit 100


# keyword: root
# description: the root DN of the CA IdentityMinder server
# value: a valid DN string
# default: dc=eta
# root dc=eta


# keyword: domain
# description: the name of the CA IdentityMinder domain
# value: a string
# default: im
# domain    im


# keyword: user
# description: the CA IdentityMinder Global User name used to bind to the CA
IdentityMinder server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin


# keyword: password
# description: the clear-text password of the "binding" CA IdentityMinder Global
User
# value: the password of the above Global User
# default: no default
password SECRET
```

```
# keyword: directory-type
# description: the CA IdentityMinder Unix Endpoint type of this Unix server
# value: ETC or NIS
# default: ETC
# endpoint-type ETC

# keyword: endpoint-name
# description: the CA IdentityMinder Unix Endpoint name of this Unix server
# value: a valid Unix Endpoint name string
# default:
# ETC: the result of the "hostname" command (ie: gethostname() system call)
# NIS: "domain [hostname]" where "domain" is the result of the "domainname" command
#  (ie: getdomainname() system call) and "hostname" the result of the "hostname"
#    command (ie: gethostname() system call)
# endpoint-name dirname

# keyword: tls-cacert-file
# description: the name of the CA IdentityMinder CA certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/et2_cacert.pem
# tls-cacert-file /etc/pam_CA_eta/et2_cacert.pem

# keyword: tls-cert-file
# description: the name of the CA IdentityMinder client certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientcert.pem
# tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem

# keyword: tls-key-file
# description: the name of the CA IdentityMinder client private key file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientkey.pem
# tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem

# keyword: tls-random-file
# description: the name of the "pseudo random number generator" seed file
# value: a valid full path file name
# default: /etc/pam_CA_eta/prng_seed
# tls-random-file /etc/pam_CA_eta/prng_seed

# keyword: use-status
# description: this module will exit with a non-zero status code in case of failure.
# value: yes or no
# default: no
# use-status no
```

```
# keyword: verbose
# description: this module will display informational or error messages to the
user.
# value: yes or no
# default: yes
# verbose yes
```

Remarque : Les paramètres de serveur, de domaine et de mot de passe n'ont pas de valeur par défaut et ne doivent pas être mis à jour.

Configuration du fichier pam.conf

Le fichier /etc/pam.conf est le principal fichier de configuration de PAM. Vous devez le modifier et insérer une ligne dans la pile de service de mots de passe. Sous certains systèmes Linux, le fichier pam.conf est remplacé par /etc/pam.d ; vous devrez donc modifier le fichier /etc/pam.d/system-auth.

Pour configurer le fichier pam.conf :

1. Accédez au répertoire /etc, ou au répertoire /etc/pam.d si vous configurez le module PAM sous un système Linux approprié.
2. Modifiez le fichier pam.conf et insérez une ligne de synchronisation de mot de passe dans la pile de service de mots de passe. Pour les configurations spécifiques aux plates-formes, consultez les exemples suivants :

   passwd password required /usr/lib/security/pam_unix.so

   passwd password optional /usr/lib/security/pam_CA_eta.so

3. (Facultatif) Vous pouvez ajouter les paramètres facultatifs suivants dans la ligne du module pam_CA_eta :

   config=/path/file

   Indique l'emplacement d'un autre fichier de configuration.

   Syslog

   Envoie des messages erreur et d'information au service syslog local.

   trace

   Génère un fichier de suivi pour chaque opération de mise à jour de mot de passe. Les fichiers de suivi sont nommés /tmp/pam_CA_eta-trace.<nnnn>, <nnnn> étant le numéro PID du processus de mot de passe.

4. Implémentez les changements de configuration spécifiques aux plates-formes suivants :

   Pour les systèmes AIX, ajoutez les lignes suivantes au bas du fichier /etc/pam.conf :

```
#
# CA IdentityMinder Unix Password Synchronization
#
login   password  optional    /usr/lib/security/pam_CA_eta.so syslog
passwd  password  optional    /usr/lib/security/pam_CA_eta.so syslog
rlogin  password  optional    /usr/lib/security/pam_CA_eta.so syslog
su      password  optional    /usr/lib/security/pam_CA_eta.so syslog
telnet  password  optional    /usr/lib/security/pam_CA_eta.so syslog
sshd    password  optional    /usr/lib/security/pam_CA_eta.so syslog
OTHER   password  optional    /usr/lib/security/pam_CA_eta.so syslog
```

   For HP-UX systems, add the following lines at the bottom of the /etc/pam.conf file:

```
#
# CA IdentityMinder Unix Password Synchronization
#
login    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
```

   For HP-UX Itanium2, add the following lines at the bottom of the /etc/pam.conf file:

```
#
# CA IdentityMinder Unix Password Synchronization
#
login    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

```
dtlogin  password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

Pour les systèmes Sun Solaris, ajoutez la ligne pam_CA_eta après la ligne pam_unix existante :

```
#

# Password management

#

other   password required       /usr/lib/security/pam_unix.so.1
other   password optional       /usr/lib/security/pam_CA_eta.so syslog
```

Pour les systèmes Linux, ajoutez la ligne pam_CA_eta entre les lignes pam_cracklib et pam_unix existantes :

```
password    required     /lib/security/pam_cracklib.so retry=3 type=
password    optional     /lib/security/pam_CA_eta.so syslog
password   sufficient   /lib/security/pam_unix.so nullok use_authtok md5 shadow
password    required     /lib/security/pam_deny.so
```

5. Pour les systèmes AIX, modifiez le fichier /etc/security/login.cfg et définissez auth_type = PAM_AUTH. Cela permet d'activer la structure PAM, qui n'est pas activée par défaut. Il s'agit d'un paramètre d'exécution qui évite de redémarrer le système pour qu'il prenne effet.

Dépannage de la synchronisation de mot de passe UNIX

Vous pouvez dépanner la fonctionnalité d'UNIX PAM à l'aide des messages Syslog et de suivi, ainsi qu'en testant la configuration, la connexion LDAP/TLS, la synchronisation de mot de passe et la structure PAM.

Informations complémentaires

Activation des messages Syslog (page 154)
Activation des messages de suivi (page 155)

Activation des messages Syslog

Ajoutez le paramètre Syslog à la ligne pam_CA_eta dans le fichier /etc/pam.conf de sorte que le module pam_CA_eta génère des messages informatifs et d'erreur. Lorsque l'option de journalisation est activée, l'administrateur UNIX voit s'afficher des messages d'informations dans les fichiers Syslog chaque fois qu'un compte UNIX change son mot de passe. Ces messages doivent fournir suffisamment d'informations pour diagnostiquer des problèmes de base.

Vous pouvez définir cette option de façon permanente dans des systèmes de production, car elle ne requiert pas davantage de ressources que lors d'une exécution du service en mode silencieux.

Activation des messages de suivi

Si les messages Syslog ne fournissent pas d'informations suffisantes, le mode de suivi peut fournir davantage de détails. Pour chaque opération de mise à jour de mot de passe, le module de suivi génère un fichier nommé /tmp/pam_CA_eta-trace.<nnnn> (<nnnn> étant le numéro PID du processus passwd) avec une entrée pour la plupart des appels de fonction utilisés par le module et les données utilisées ou renvoyées par ces fonctions.

Même si les fichiers de suivi sont lisibles uniquement par le compte racine, ils contiendront les mots de passe nouveaux en texte clair. C'est pourquoi ce paramètre ne doit pas être utilisé de façon permanente sur un système de production.

Test du fichier de configuration

Pour vérifier le fichier de configuration, vous pouvez utiliser l'outil test_config, situé dans le répertoire /etc/pam_CA_eta. Configurez d'abord la structure de répertoires comme suit :

1. Déplacez le dossier pam_CA_eta sous /etc.
2. Copiez tous les éléments sous pam_CA_eta-1.1 vers /etc/pam_CA_eta.

Voici un exemple d'entrée de ligne de commande :

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

Voici un exemple de session :

```
./test_config [config=/path/to/config_file]
#./test_config
./test_config: succeeded
Trace file is /tmp/test_config-trace.1274
```

Comme l'illustre le résultat de la commande, un fichier de suivi a été généré et contient tous les détails de l'analyse du fichier de configuration.

Affichage du service CAM

Pour connaître l'utilisateur ayant lancé le service, vous pouvez appliquer la procédure suivante.

Pour afficher le service CAM :

1. Connectez-vous à l'ordinateur UNIX en tant qu'utilisateur root à l'aide du client Telnet ou SSH.
2. Emettez la commande UNIX suivante :

   ```
   ps -ef | grep cam
   ```

   Un affichage similaire au suivant apparaît :

   ```
   root 13822       1 11 11:30:12 ?   0:00 cam

   root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
   ```

Remarque : Si l'utilisateur root du système ne lance pas les services, ils apparaîtront comme démarrés, mais vous ne serez pas en mesure de les utiliser. CA IdentityMinder émet le message suivant : Permission denied: user must be root (Autorisation refusée : l'utilisateur doit être un utilisateur root).

Test de la connexion LDAP/TLS

Pour vérifier la connexion au serveur de provisionnement, à l'aide des paramètres du fichier de configuration, vous pouvez utiliser l'outil test_ldap, situé dans le répertoire /etc/pam_CA_eta. Voici un exemple d'entrée de ligne de commande :

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

Voici un exemple de session :

```
./test_ldap [config=/path/to/config_file]
# ./test_ldap: succeeded
Trace file is /tmp/test_ldap-trace.1277
```

Comme l'illustre le résultat de la commande, un fichier de suivi a été généré et contient tous les détails de l'analyse du fichier de configuration et de la connexion au serveur de provisionnement.

Test de la synchronisation du mot de passe

Pour vérifier que la mise à jour du mot de passe d'un compte local est correctement propagée par le serveur de provisionnement, vous pouvez utiliser l'outil test_sync, situé dans le dossier /etc/pam_CA_eta. Voici un exemple d'entrée de ligne de commande :

```
/etc/pam_CA_eta/test_sync <user> <password> [config=/path/to/config_file]
```

Voici un exemple de session :

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
CA IdentityMinder password synchronization started.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
CA IdentityMinder password synchronization succeeded.
/etc/pam_CA_eta/test_sync: succeeded
Trace file is /tmp/test_sync-trace.2244
```

Comme l'illustre le résultat de la commande, un fichier de suivi a été généré et contient tous les détails de l'analyse du fichier de configuration, de la connexion au serveur de provisionnement et de la mise à jour du compte.

Lors de l'utilisation du mode détaillé (à l'aide du paramètre par défaut verbose yes dans le fichier de configuration), la commande fournit des messages informatifs et d'erreur potentiels sur la propagation de mot de passe.

Test de la structure PAM

Une bibliothèque de test PAM est disponible pour vérifier que les modifications de mot de passe sont correctement détectées par la structure PAM.

Pour tester la structure PAM :

1. Copiez le fichier pam_test dans le dossier /usr/lib/security(/hpux32).
2. Ajoutez une ligne de classe de mot de passe pour la bibliothèque pam_test sans paramètres.

   Voici un exemple pour Solaris :

   ```
   other password optional /usr/lib/security/pam_test
   ```

3. Emettez une commande passwd sur un utilisateur test, puis recherchez la ligne marquée pam_test[<pid>] dans le fichier Syslog.

   Le résultat de la commande indique le nom du fichier de suivi généré, par exemple :

   ```
   pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
   ```

Passwords on OS400

L'agent de synchronisation du mot de passe permet la propagation des modifications de mot de passe apportées sur le système de terminal OS/400, vers les autres comptes gérés par CA IdentityMinder. L'agent de synchronisation du mot de passe fonctionne comme suit :

1. Installation et exécution de l'agent sur le système de terminal OS/400

   Dans le cadre de l'installation, le programme est enregistré auprès du système OS/400 de sorte que lorsque les utilisateurs changent leurs mots de passe, l'agent renvoie ces modifications au serveur de provisionnement.

2. Le serveur de provisionnement propage la modification de mot de passe aux comptes associés.

   Les modifications de mot de passe initialisées à partir de la commande de modification de mots de passe (CHGPWD) ou de l'API de modification de mots de passe (QSYCHGPW) sont reçues par l'agent.

3. L'agent journalise la réussite ou l'échec de l'opération dans un fichier journal situé sous PWDSYNCH/LOG.

L'agent de synchronisation du mot de passe est pris en charge sur les plates-formes suivantes :

- OS400 V5R2
- OS400 V5R3
- OS400 V5R4

Pour installer l'agent de synchronisation du mot de passe :

1. Recherchez le média d'installation du composant de provisionnement.
2. Exécutez le programme d'installation de l'agent de synchronisation du mot de passe ou OS/400 sous \Agent
3. Pour effectuer l'installation, suivez les instructions à l'écran.

   Remarque : Les instructions d'installation dans le lien du logiciel de l'agent du terminal sont décrites dans les sections suivantes.

Installation de l'agent de synchronisation du mot de passe OS400

Vous devez disposer des droits *ADDOBJ et les conditions suivantes sont nécessaires à la réception des notifications de modification du mot de passe par l'agent :

- La valeur système QPWDVLDPGM doit être définie sur *REGFAC.
- Le programme doit être enregistré avec la commande WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD).
- L'environnement doit autoriser la provenance des modifications de mot de passe à partir des comptes de terminal. Un administrateur disposant d'un accès à la console de gestion active cette fonctionnalité.

L'agent est initialisé uniquement lors d'une modification de mot de passe. Pour changer le mot de passe, émettez la commande CHGPWD.

Remarque : L'utilisateur global doit être marqué pour la synchronisation du mot de passe.

Sous iSeries

1. Connectez-vous en tant qu'utilisateur disposant des droits *ALLOBJ et *SECADM (par exemple, QSECOFR).
2. Créez un utilisateur appelé PWDSYNCH :

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   Remarque : Par mesure de sécurité, l'utilisateur est créé avec le mot de passe expiré.
3. Créez un fichier de sauvegarde pour stocker le package d'installation dans une bibliothèque de votre choix (par exemple : MYLIB) :

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```
4. Sur l'ordinateur Windows contenant le fichier de sauvegarde, utilisez FTP pour transférer ce fichier vers iSeries :

   ```
   ftp <nom_hôte>
   binaire
   cd MYLIB
   put PWDSYNCH.FILE
   ```
5. Sur iSeries, extrayez le programme du fichier de sauvegarde :

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   Cette commande permet d'extraire et d'installer l'agent de synchronisation dans la bibliothèque PWDSYNCH.
6. Vérifiez l'installation :

   ```
   DSPLIB PWDSYNCH
   ```

   Les objets suivants doivent s'afficher :

Objet	Type	Attribut
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. Configurez iSeries pour utiliser PWDSYNCH comme programme de sortie de la validation de mot de passe :

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. Sous iSeries, spécifiez les paramètres de connexion de votre serveur de connecteurs CA IAM :

```
EDTF FILE(PWDSYNCH/CONFIG)
```

Installation de l'agent de synchronisation du mot de passe OS400

Vous devez disposer des droits *ADDOBJ et les conditions suivantes sont nécessaires à la réception des notifications de modification du mot de passe par l'agent :

- La valeur système QPWDVLDPGM doit être définie sur *REGFAC.
- Le programme doit être enregistré avec la commande WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD).
- L'environnement doit autoriser la provenance des modifications de mot de passe à partir des comptes de terminal. Un administrateur disposant d'un accès à la console de gestion active cette fonctionnalité.

L'agent est initialisé uniquement lors d'une modification de mot de passe. Pour changer le mot de passe, émettez la commande CHGPWD.

Remarque : L'utilisateur global doit être marqué pour la synchronisation du mot de passe.

Sous iSeries

1. Connectez-vous en tant qu'utilisateur disposant des droits *ALLOBJ et *SECADM (par exemple, QSECOFR).
2. Créez un utilisateur appelé PWDSYNCH :

```
CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
```

Remarque : Par mesure de sécurité, l'utilisateur est créé avec le mot de passe expiré.

3. Créez un fichier de sauvegarde pour stocker le package d'installation dans une bibliothèque de votre choix (par exemple : MYLIB) :

```
CRTSAVF MYLIB/PWDSYNCH
```

4. Sur l'ordinateur Windows contenant le fichier de sauvegarde, utilisez FTP pour transférer ce fichier vers iSeries :

```
ftp <nom_hôte>
binaire
cd MYLIB
put PWDSYNCH.FILE
```

5. Sur iSeries, extrayez le programme du fichier de sauvegarde :

```
RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
```

Cette commande permet d'extraire et d'installer l'agent de synchronisation dans la bibliothèque PWDSYNCH.

6. Vérifiez l'installation :

```
DSPLIB PWDSYNCH
```

Les objets suivants doivent s'afficher :

Objet	Type	Attribut
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. Configurez iSeries pour utiliser PWDSYNCH comme programme de sortie de la validation de mot de passe :

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. Sous iSeries, spécifiez les paramètres de connexion de votre serveur de connecteurs CA IAM (CA IAM CS) :

```
EDTF FILE(PWDSYNCH/CONFIG)
```

Mise à jour du terminal dans la console d'utilisateur

Dans la console d'utilisateur, mettez à jour le terminal pour indiquer que l'agent est installé.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur.
2. Cliquez sur Terminaux, Gérer les terminaux, Modifiez le terminal.
3. Recherchez le terminal sur lequel l'agent est installé.
4. Cliquez sur l'onglet Paramètres du terminal.
5. Sélectionnez la case à cocher Agent de synchronisation du mot de passe installé.

Activation d'un environnement pour la synchronisation de mot de passe

Après avoir installé l'agent de synchronisation du mot de passe, vous devez autoriser l'environnement à recevoir les modifications de mot de passe appliquées aux terminaux. Pour cette tâche, un administrateur requiert l'accès à la console de gestion et à CA Directory pour permettre à l'environnement d'accepter ces modifications.

Procédez comme suit:

1. Pour les nouveaux utilisateurs, utilisez la console de gestion comme suit :
   a. Sélectionnez l'environnement.
   b. Cliquez sur Advanced Settings (Paramètres avancés), Provisonning (Provisionnement).
   c. Sélectionnez la case à cocher Enable Password Changes (Activer les modifications de mot de passe) sous Endpoint Accounts (Comptes de de terminal).
2. Pour les utilisateurs existants, définissez l'attribut eTPropagatePassword sur 1 dans CA Directory.

Configuration SSL

SSL est utilisé pour chiffrer la communication entre l'agent de synchronisation et le serveur de provisionnement. Cela est important pour l'agent de synchronisation, car SSL envoie des mots de passe via le réseau. Il est recommandé d'utiliser SSL.

L'agent de synchronisation doit approuver le certificat du serveur de provisionnement afin de se connecter à SSL. Par conséquent, le certificat doit être installé sur l'ordinateur iSeries et configuré de sorte que l'agent de synchronisation approuve le certificat. Ces tâches sont effectuées par le gestionnaire de certificats numériques (Digital Certificate Manager, DCM), un composant facultatif de OS/400. Consultez la documentation de OS/400 concernant l'installation et l'installation du gestionnaire de certificats numériques.

Installation du certificat de serveur de provisionnement

Pour utiliser SSL, les composants de système d'exploitation suivants doivent être installés sur votre ordinateur iSeries :

- Programme cryptographique autorisé sous licence par un fournisseur d'accès (5722 AC3)
- Gestionnaire de certificats numériques (Option 34 de OS/400)
- Serveur HTTP IBM pour iSeries (5722 DG1)

Sous iSeries

1. Chargez le certificat de serveur de provisionnement à partir de l'ordinateur du serveur de provisionnement vers iSeries. Vous pouvez trouver le certificat à l'emplacement suivant :

   ```
   C:\Program Files\CA\Identity Manager\Provisioning
   Server\Data\Tls\server\et2_cacert.pem
   ```

2. Connectez-vous au DCM.

   A l'aide d'un navigateur Web, accédez à http://<nom d'hôte>:2001. Lorsque vous y êtes invité, connectez-vous en tant qu'utilisateur QSECOFR et cliquez sur le lien du gestionnaire de certificats numériques.

3. Utilisez le référentiel de certificats *SYSTEM.

   Cliquez sur Select a Certificate Store (Sélectionner un référentiel de certificats) et sélectionnez le référentiel de certificats *SYSTEM. S'il n'existe pas, créez un référentiel appelé *SYSTEM, puis saisissez le mot de passe du référentiel de certificats.

4. Importez le certificat en tant que certificat d'autorité de certification à l'aide du DCM.

   Cliquez sur Manage Certificates (Gérer des certificats), Importer des certificats et sélectionnez Autorité de certification (CA), puis saisissez le nom du fichier de certificat du serveur de provisionnement. Il s'agit de l'emplacement où vous avez chargé le certificat à l'étape 1. Saisissez l'étiquette Serveur de provisionnement pour le certificat.

   L'importation du certificat est terminée.

5. A l'issue de l'importation du certificat d'autorité de certification dans le référentiel de clés *SYSTEM du terminal, veillez à ce que le client IBM Directory QIBM_GLD_DIRSRV_CLIENT puisse accéder au référentiel de clés *SYSTEM. Sans quoi, l'appel d'initialisation SSL de l'agent de synchronisation du mot de passe échouera.

6. Pour configurer l'application Directory Services client (client de services d'annuaire) de sorte à approuver le certificat du serveur de provisionnement, ouvrez Manage Applications (Gérer des applications), Define CA trust list (Définir la liste de confiance d'autorité de certification) et sélectionnez Directory Services client (client de services d'annuaire).

   Si l'importation s'est correctement effectuée à l'étape 4, le certificat du serveur de provisionnement doit être répertorié ici.

   Cliquez sur Trusted (fiable) pour le certificat du serveur de provisionnement et cliquez sur OK au bas de la liste.

7. Accordez des autorisations de lecture publique aux fichiers SSL et des droits d'accès en lecture au référentiel de certificats *SYSTEM :

   ```
   (/QIBM/userdata/ICSS/Cert/Server/default.kdb)
   ```

   Accordez des autorisation de lecture et d'exécution au dossier parent :

   ```
   (/QIBM/userdata/ICCS/Cert/Server)
   ```

   Remarque : L'adoption de l'autorité de l'utilisateur PWDSYNCH ne fonctionne pas dans le système de fichiers / ; l'accès doit donc être accordé à tous les utilisateurs.

Désinstallation de l'agent de synchronisation du mot de passe

Si vous devez désinstaller l'agent de synchronisation du mot de passe, suivez la procédure suivante.

A partir du point de sortie de la validation de mot de passe :

1. Supprimez PWDSYNCH :

   ```
   RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   ```

2. Supprimez la bibliothèque de l'agent de synchronisation :

   ```
   DLTLIB PWDSYNCH
   ```

3. Supprimez l'utilisateur PWDSYNCH :

   ```
   DLTUSRPRF PWDSYNCH
   ```

4. Supprimez le certificat du serveur de provisionnement en suivant les instructions SSL pour vous connecter au DCM et utilisez le référentiel de certificats *SYSTEM :

   Cliquez sur Manage Certificates (Gérer les certificats), Delete Certificate (Supprimer un certificat) et sélectionnez Autorité de certification (CA).

   Sélectionnez le certificat Serveur de provisionnement et cliquez sur Supprimer.

Le paramètre de l'agent de mot de passe OS/400 doit être correctement défini

La valeur du paramètre pwd_case_action doit être définie correctement pour que le paramètre fonctionne. Les valeurs correctes sont indiquées ci-après.

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

Si pwd_case_action = [valeur non valide], le mot de passe est obligatoirement en majuscules.

Remarque : Lors de la configuration de l'agent de synchronisation du mot de passe, notez la valeur système QPWDLVL (niveau du mot de passe).

- Si QPWDLVL est définie sur 0 (valeur par défaut) dans le système AS400, les mots de passe de 1 à 10 caractères en majuscule sont pris en charge.
- Si QPWDLVL est définie sur 2 ou 3, les mots de passe de 1 à 128 caractères en majuscule et minuscule sont autorisés.

Par défaut, l'agent de synchronisation du mot de passe propage le mot de passe inchangé au serveur de provisionnement. Toutefois, indépendamment de la valeur de QPWDLVL, vous pouvez forcer l'agent de synchronisation du mot de passe à propager des mots de passe en majuscule ou minuscule en définissant pwd_case_action sur pwd_to_uppercase ou pwd_to_lowercase respectivement.

Chapitre 7: Groupes

Vous pouvez créer différents types de groupes ou en combiner plusieurs :

- Groupe statique : une liste des utilisateurs qui sont ajoutés de manière interactive
- Groupe dynamique : les utilisateurs appartiennent à ce groupe s'ils remplissent une requête LDAP (nécessite un annuaire LDAP comme magasin d'utilisateurs)

  Remarque : Le champ Requête de groupe dynamique n'est pas inclus dans la tâche Créer un groupe ou dans les tâches d'un autre groupe, même si ce champ existe dans le répertoire.xml pour un groupe. Vous incluez le champ Requête de groupe dynamique dans la tâche en modifiant l'écran du profil associé.

- Groupe imbriqué : un groupe contenant d'autres groupes (nécessite un annuaire LDAP comme magasin d'utilisateurs)

Remarque : Pour afficher les groupes statiques, dynamiques et imbriqués auxquels appartient un utilisateur, utilisez l'onglet Groupe pour l'objet Utilisateur. Cet onglet apparaît par défaut dans les tâches Afficher et modifier des utilisateurs.

Ce chapitre traite des sujets suivants :

Création d'un groupe statique

Vous pouvez associer un ensemble d'utilisateurs à un *groupe statique*. Vous gérez le groupe statique en ajoutant ou supprimant des utilisateurs individuels de la liste d'appartenance à un groupe. Pour afficher la liste des membres d'un groupe, utilisez l'onglet Appartenance, qui est inclus par défaut dans les tâches Afficher et modifier un groupe.

Remarque : L'onglet Appartenance affiche uniquement les membres ajoutés de manière explicité au groupe. Il n'affiche pas les membres qui sont ajoutés dynamiquement.

Pour créer un groupe statique :

1. Dans la console d'utilisateur, sélectionnez Groupes, puis Créer un groupe.
2. Choisissez de créer un nouveau groupe ou d'en copier un, puis cliquez sur **OK**.

3. Dans l'onglet Profil, saisissez un nom de groupe, une organisation de groupe, une description et un nom d'administrateur de groupe.
4. Cliquez sur l'onglet Appartenance.
5. Cliquez sur Ajouter un utilisateur
6. Cherchez des utilisateurs à inclure dedans.
7. Mettez une coche en regard des utilisateurs et cliquez sur Sélectionner.
8. Cliquez sur Soumettre.

Création d'un groupe dynamique

Vous pouvez créer un *groupe dynamique* en définissant une requête de filtrage LDAP au moyen de la console d'utilisateur, afin de déterminer de manière dynamique l'appartenance au groupe au moment de l'exécution, sans avoir à rechercher et à ajouter individuellement des utilisateurs.

Par exemple, si vous souhaitez générer un groupe qui répertorie tous les employés de NeteAuto aux Etats-Unis, vous pouvez définir un filtre de recherche LDAP similaire au suivant dans le champ Requête de groupe dynamique de la console d'utilisateur :

ldap:///cn=Employés,o=NeteAuto,c=US??sub

Vous pouvez également modifier cette requête pour localiser les employés en dehors des Etats-Unis.

La rubrique Exemple de groupes statiques, dynamiques et imbriqués (page 173) présente un exemple de groupe créé par des groupes statiques, dynamiques et imbriqués.

Remarque : Pour inclure le champ Requête de groupe dynamique dans la tâche, modifiez la fenêtre du profil associé. Il n'est pas inclus par défaut dans la tâche Créer un groupe.

Pour créer un groupe dynamique :

1. Dans la console d'utilisateur, sélectionnez Groupes, puis Créer un groupe.
2. Choisissez de créer un nouveau groupe ou d'en copier un, puis cliquez sur **OK**.
3. Dans l'onglet Profil, saisissez un nom de groupe, une organisation de groupe, une description et un nom d'administrateur de groupe.

4. Saisissez un filtre de recherche LDAP comme l'exemple suivant dans le champ Requête de groupe dynamique :

   ldap:///cn=Employés,o=NeteAuto,c=US??sub

5. Cliquez sur Soumettre.

Remarque : Seul un administrateur avec la tâche Modifier le groupe peut changer une appartenance à un groupe dynamique.

Paramètres de requête de groupe dynamique

Vous pouvez utiliser dans la recherche les paramètres de requête dynamique suivants.

ldap:///*<DN_base recherche>*??*<portée_recherche>*?*<filtrerecherche>*

- *<DN_base_recherche>* représente le point à partir duquel vous commencez la recherche dans l'annuaire LDAP. Si vous n'indiquez pas le DN de base dans la requête, l'organisation du groupe correspond alors au DN de base par défaut.
- *<portée_recherche>* spécifie l'étendue de la recherche et inclut les paramètres suivants.
  - sub : renvoie les entrées au niveau du DN de base et en dessous.
  - one : renvoie les entrées un niveau au-dessous du DN de base spécifié dans l'URL. (action par défaut).
  - base : utilise "one" et ignore "base" comme recherche d'option.

  Les valeurs "one" ou "base" renvoient uniquement les utilisateurs de l'organisation du nom unique de base.

  La valeur "sub" renvoie tous les utilisateurs sous l'organisation du DN de base et toutes les sous-organisations de l'arborescence.

- *<filtrerecherche>* est le filtre que vous souhaitez appliquer aux entrées figurant dans la portée de la recherche. Quand vous saisissez un filtre de recherche, utilisez la syntaxe standard de requête LDAP comme indiqué ci-après.

  (<opérateur_logique><comparaison><comparaison...>)

  - <opérateur logique> correspond à l'une des valeurs suivantes.

    OU logique : |

    ET logique : &

    NON logique : !

  - <comparaison> indique <attribut><opérateur><valeur>

  Exemple :

  (&(ville=boston)(état=Massachusetts))

  Le filtre de recherche par défaut est (objectclass=*).

Lors de la création d'une requête dynamique, tenez compte des conditions suivantes :

- Le préfixe "ldap" doit figurer en minuscule, par exemple :

  ldap:///o=MaSociété??sub?(titre=Gestionnaire)

- Vous ne pouvez pas spécifier le nom d'hôte ou le numéro de port du serveur LDAP. Toutes les recherches se produisent dans l'annuaire LDAP qui est associé à l'environnement.

Le tableau suivant inclut des requêtes LDAP d'exemple :

Description	**Requête**
Tous les utilisateurs qui sont gestionnaires	ldap:///o=MaSociété??sub?(titre=Gestionnaire)
Tous les gestionnaires de la succursale de New York	ldap:///o=MaSociété??one?(&(titre=Gestionnaire) (roomNumber=NYWest))
Tous les techniciens disposant d'un téléphone portable	ldap:///o=MaSociété??one? (&(employeetype=technicien) (Portable=*))
Tous les employés dont le matricule est compris entre 1000 et 2000	ldap:///o=MaSociété, (& (ou=employé) (employeenumber >=1000) (employeenumber <=2000))
Tous les administrateurs du centre d'assistance qui sont employés par la société depuis plus de 6 mois	ldap:///o=MaSociété,(& (cn=helpdeskadmin) (DEMB => 2004/04/22) **Remarque :** Cette requête nécessite la création d'un attribut DEMB pour la date d'embauche de l'utilisateur.

Remarque : Les comparaisons > et < (supérieur à et inférieur à) sont lexicographiques et non arithmétiques. Pour des informations plus détaillées sur leur utilisation, reportez-vous à la documentation de votre serveur d'annuaire LDAP.

Création d'un groupe imbriqué

Si le magasin d'utilisateurs se trouve dans un annuaire LDAP, vous pouvez ajouter un groupe en tant que membre d'un autre groupe. Le groupe est appelé un *groupe imbriqué*.

Le groupe contenant le groupe imbriqué est appelé un *groupe parent*. Les membres du groupe imbriqué deviennent membres du groupe parent. Cependant, les membres du groupe parent ne deviennent pas membres d'un groupe imbriqué.

Les groupes imbriqués ressemblent aux listes de diffusion par courriel où une liste peut être membre d'une autre. Avec les groupes imbriqués, vous pouvez ajouter des groupes et des utilisateurs en tant que membres dans le groupe. En imbriquant un groupe dans une autre liste d'appartenance de groupes, vous pourriez inclure tous les membres des groupes imbriqués.

Par exemple, si vous avez créé des groupes séparés pour les services fabrication, conception, expédition et comptabilité d'une société, vous pouvez construire un groupe parent pour la société toute entière, en imbriquant tous les groupes de services séparés en tant que membre du groupe parent. Par conséquent, toutes les modifications apportées aux groupes imbriqués de fabrication, conception, expédition et comptabilité se reflèteraient automatiquement dans le groupe imbriqué pour la société entière. Un groupe imbriqué dans un autre groupe peut être dynamique et/ou contenir d'autres groupes imbriqués.

La capture de l'exemple de groupes statiques, dynamiques et imbriqués (page 173) montrer un groupe parent créé par des groupes statiques, dynamiques et imbriqués.

Tenez compte du conseil suivant avant de créer un groupe imbriqué :

- Seul un administrateur avec une tâche Modifier les membres du groupe peut ajouter ou modifier les groupes imbriqués à partir de la liste de membres statiques du groupe dans la console d'utilisateur.
- Seuls les utilisateurs avec les droits d'administrateur correspondants peuvent modifier, ajouter ou supprimer des membres dans un groupe.

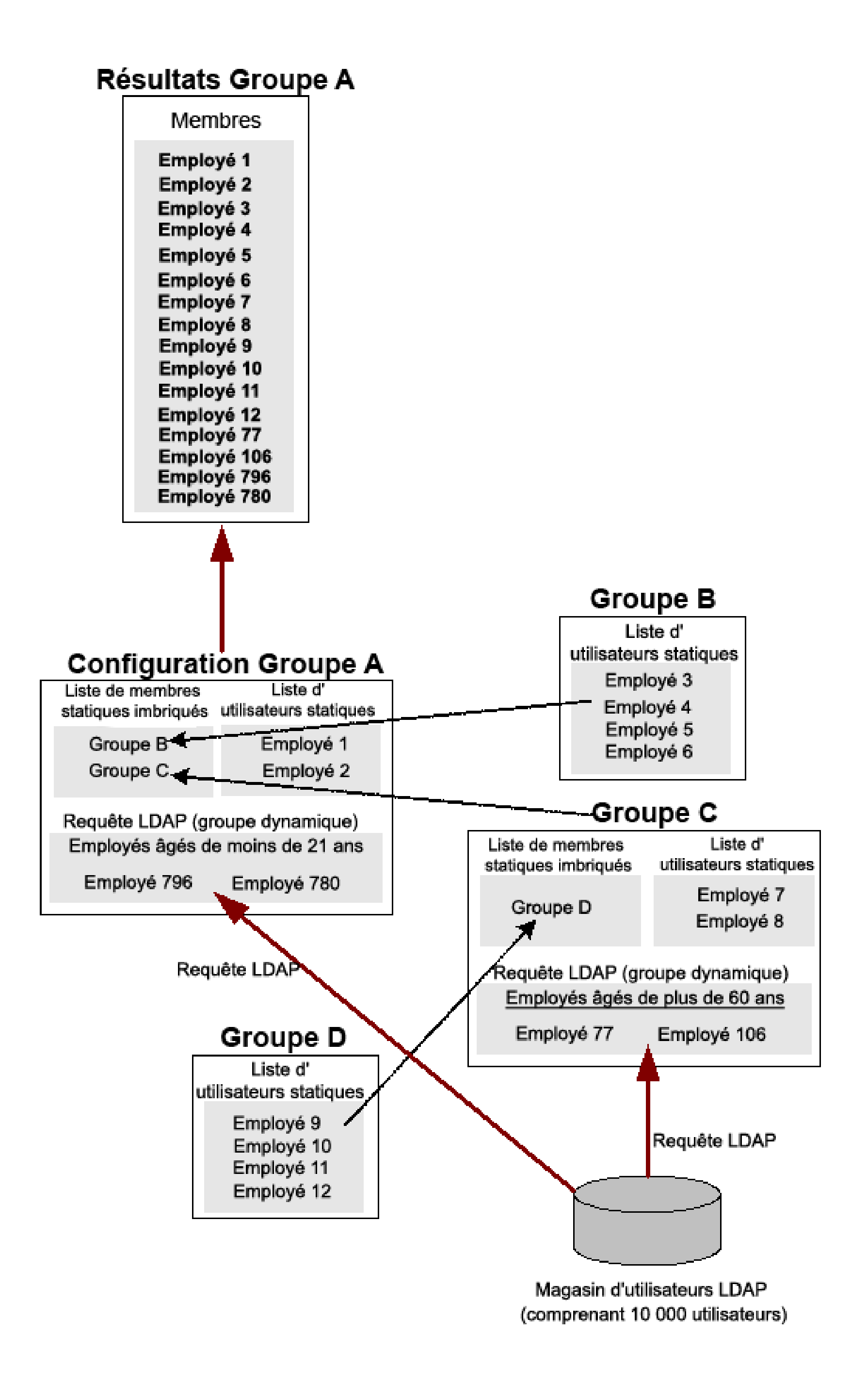
  Par exemple, si le groupe parent A est créé par les groupes imbriqués B et C, l'administrateur du groupe A peut uniquement modifier les membres du groupe A mais pas B et C. Les groupes B et C peuvent seulement être modifiés par leurs administrateurs respectifs.

Pour créer un groupe imbriqué :

1. Dans la console d'utilisateur, sélectionnez Groupes, puis Créer un groupe.
2. Choisissez de créer un nouveau groupe ou d'en copier un, puis cliquez sur **OK**.
3. Dans l'onglet Profil, saisissez un nom de groupe, une organisation de groupe, une description et un nom d'administrateur de groupe.
4. Dans l’onglet Appartenance :
   a. Cliquez sur Ajouter un groupe pour ajouter un groupe imbriqué dans ce groupe.
   b. Recherche d'un groupe existant.
   c. Mettez une coche en regard du groupe et cliquez sur Sélectionner.
   d. Cliquez sur Soumettre.

Exemple de groupes statiques, dynamiques et imbriqués

Les groupes peuvent être complexes et consister en une combinaison de groupes statiques, dynamiques ou imbriqués. La capture ci-après est un exemple de groupe créé à partir de groupes statiques, dynamiques et imbriqués.



Dans la capture précédente :

- Le groupe parent A contient des groupes imbriqués B et C, deux utilisateurs statiques et une requête LDAP dynamique listant tous les employés âgés de moins de 21 ans.
- Le groupe B est composé de quatre utilisateurs statiques.
- Le groupe parent C contient le groupe imbriqué D et une requête LDAP dynamique listant tous les employés âgés de plus de 60 ans.
- Le groupe D contient quatre utilisateurs statiques.
- La partie supérieure de la capture liste les membres du groupe A, qui proviennent des groupes imbriqués, des requêtes dynamiques et des listes de membres d'utilisateurs statiques des groupes B, C et D.

Administrateurs de groupes

Dans l'onglet Administrateurs des tâches Créer ou Modifier un groupe, vous pouvez spécifier des utilisateurs et des groupes en tant qu'administrateurs d'un groupe. Lorsque vous affectez un utilisateur en tant qu'administrateur de groupe, assurez-vous que l'administrateur a un rôle d'une portée appropriée pour gérer le groupe. Par exemple :

1. Utilisation de Modifier un groupe pour affecter un utilisateur en tant qu'administrateur de groupe.
2. Affectation de cet utilisateur au rôle d'administrateur avec des tâches de gestion de groupe, comme Modifier les membres du groupe, ou des tâches de gestion des utilisateurs avec un onglet Groupe.
3. Vérifiez que le rôle a une portée appropriée par rapport au groupe.
    a. Utilisez Afficher le rôle d'administration sur le rôle auquel vous affectez des tâches de gestion de groupe.
    b. Dans l'onglet Membres, assurez-vous qu'il existe une stratégie incluant les éléments suivants :

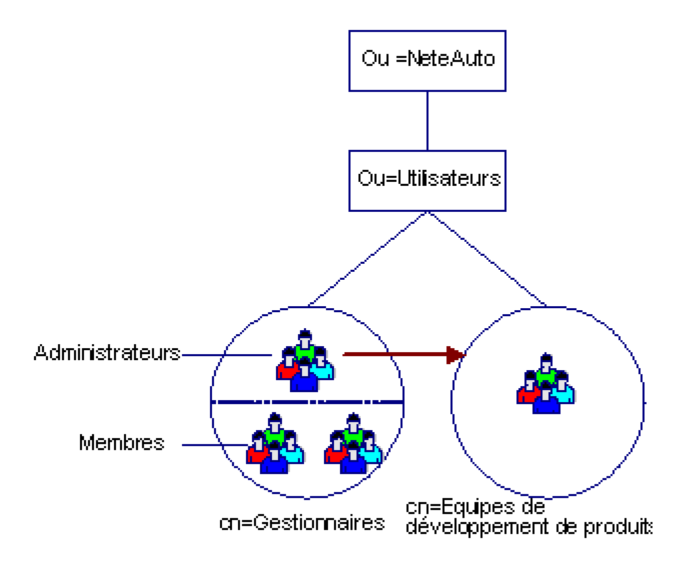
        Une règle de membres que l'administrateur du groupe respecte

        Une règle d'une portée incluant le groupe

        Une règle d'une portée incluant quelques utilisateurs à ajouter au groupe

Remarque : Pour activer des groupes en tant qu'administrateurs d'autres groupes dans un environnement IdentityMinder, configurez la prise en charge de l'administrateur de groupe dans le fichier de configuration de l'annuaire. Pour plus d'informations, reportez-vous au *manuel de configuration*.

Lorsque vous affectez un groupe en tant qu'administrateur, seuls les administrateurs de ce groupe seront les administrateurs du groupe que vous créez ou modifiez. Les membres du groupe d'administrateurs que vous spécifiez n'auront pas les droits de gestion du groupe. L'illustration suivante montre un groupe en tant qu'administrateur d'un autre groupe.



Dans cet exemple :

- Le Responsable du groupe est un administrateur du groupe Product Teams.
- Les administrateurs des Responsables peuvent gérer le groupe Product Teams. Les membres du groupe des Responsables ne peuvent pas.

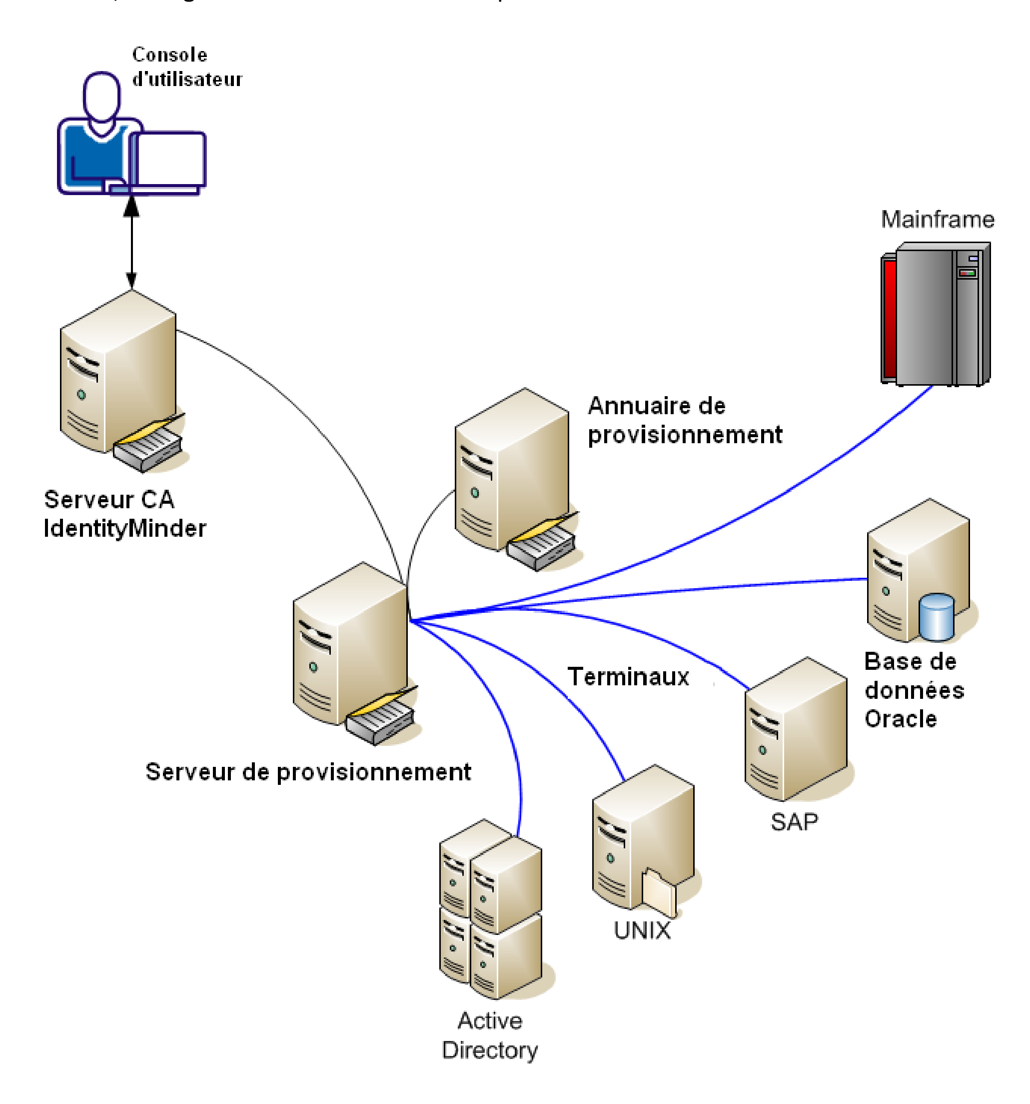
Chapitre 8: Comptes de terminaux gérés

CA IdentityMinder permet de gérer des comptes sur des terminaux si votre installation de CA IdentityMinder dispose d'un serveur de provisionnement. Vous pouvez gérer des comptes (par exemple, Exchange, Windows NT ou Oracle) ainsi que des comptes orphelins et système qui ne sont pas actuellement associés à CA IdentityMinder.

Ce chapitre traite des sujets suivants :

Intégration de terminaux gérés

Avec CA IdentityMinder, vous pouvez gérer des comptes sur plusieurs systèmes à partir d'une interface utilisateur unique : la console d'utilisateur. Les comptes se trouvent sur des systèmes qui sont envoyés vers des terminaux gérés ou simples. Dans l'exemple suivant, vous gérez des utilisateurs sur cinq terminaux.



Vous pouvez affecter des comptes à un utilisateur sur tous les types de combinaison de terminaux. Lorsque vous intégrez un terminal, CA IdentityMinder associe chaque compte de terminal à un utilisateur de l'annuaire de provisionnement.

Les procédures suivantes décrivent la procédure d'intégration des terminaux pour permettre la gestion des comptes de terminaux à partir de la console d'utilisateur.

1. Importation du fichier de définition de rôle (page 179)
2. Création de règles de corrélation (page 179)
3. Ajout du terminal à l'environnement (page 182)
4. Création d'une définition d'exploration et de corrélation (page 182)
5. Exploration et corrélation d'un terminal (page 184)

Importation du fichier de définition de rôle

Vous importez les définitions de rôle d'un fichier qui s'applique au nouveau terminal. Cette procédure requiert l'accès à la console de gestion.

Procédez comme suit:

1. Dans la console de gestion, cliquez sur Environnements.
2. Sélectionnez l'environnement dans lequel vous ajoutez le terminal.
3. Cliquez sur les paramètres Rôle et Tâche.
4. Cliquez sur Importer.
5. Sélectionnez un terminal dans Type de terminal.
6. Cliquez sur Terminer.

   Le statut de l'importation s'affiche dans la fenêtre actuelle.
7. Cliquez sur Continuer pour sortir.
8. Redémarrez l'environnement pour appliquer les modifications.

Création de règles de corrélation

Un administrateur d'hébergement ou un administrateur avec la tâche Configurer les attributs de corrélation peut créer des règles qui sont utilisées lorsque vous explorez un terminal. La tâche Exécuter la corrélation et l'exploration utilise ces règles pour la partie de corrélation de la tâche.

Les règles de corrélation déterminent la manière dont un attribut de compte de terminal est mappé vers un attribut d'utilisateur dans la console d'utilisateur. Par exemple, Access Control contient un attribut nommé AccountName. Vous pouvez créer une règle pour le mapper vers FullName dans la console d'utilisateur. Si les règles impliquent l'application de deux mappages vers un attribut d'utilisateur, la première valeur de paramètre est utilisée.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur.
2. Cliquez sur Système, Configuration du provisionnement, Configurer les attributs de corrélation.
3. Cliquez sur Ajouter.
4. Définissez une règle de corrélation comme suit :
    a. Sélectionnez une liste d'attributs de l'utilisateur global.

       Cette valeur fait référence à l'attribut d'utilisateur répertorié dans l'annuaire de provisionnement.
    b. Activez la case à cocher Définir un attribut de compte spécifique.
    c. Sélectionnez un type de terminal.
    d. Sélectionnez un attribut de compte qui s'applique à l'attribut de l'utilisateur global.
    e. Vous pouvez également remplir les champs Sous-chaîne.

       Si le champ Sous-chaîne d'origine est vide, le traitement commence au début de la chaîne. Si le champ Sous-chaîne cible est vide, le traitement commence à la fin de la chaîne.
5. Cliquez sur OK.
6. Cliquez sur Soumettre.

Remarque : Chaque fois que vous modifiez une règle de corrélation, explorez le terminal même si vous l'avez déjà exploré auparavant.

Exemple de règles de corrélation

L'exemple suivant fournit des paramètres d'exemple pour un terminal Active Directory.

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
 CustomField01=ActiveDirectory:Telephone
```

Les actions suivantes ont lieu pour chaque compte auparavant non corrélé et trouvé lors de la corrélation des comptes dans un conteneur Active Directory :

1. Le serveur de provisionnement compare la première valeur de paramètre (GlobalUserName) avec l'attribut de compte de terminal Active Directory (NT_AccountID). Le serveur tente de trouver l'utilisateur global unique dont le nom correspond à la valeur de l'attribut NT_AccountID pour ce compte. Si une correspondance unique est trouvée, le serveur de provisionnement associe le compte à l'utilisateur global. Si plusieurs correspondances sont trouvées, le serveur de provisionnement procède à l'étape 5. Si aucune correspondance n'est trouvée, le serveur de provisionnement procède à l'étape suivante.
2. Le serveur de provisionnement considère la seconde valeur de paramètre (FullName=LDAP Namespace:globalFullName). Comme cette valeur est spécifique d'un autre type de terminal, elle est ignorée et le serveur de provisionnement procède à l'étape suivante.
3. Le serveur de provisionnement considère la troisième valeur de paramètre (FullName=ActiveDirectory:DisplayName). Comme cette valeur est spécifique d'Active Directory, elle est utilisée. Le serveur tente de trouver l'utilisateur global unique dont le nom complet FullName correspond à la valeur de l'attribut DisplayName pour ce compte. Si une correspondance unique est trouvée, le serveur de provisionnement associe le compte à l'utilisateur global. Si plusieurs correspondances sont trouvées, le serveur de provisionnement procède à l'étape 5. Si aucune correspondance n'est trouvée, le serveur de provisionnement procède à l'étape 4.
4. Le serveur de provisionnement considère la valeur de paramètre finale (CustomField01=ActiveDirectory:Telephone). Comme cette valeur est spécifique d'Active Directory, elle est utilisée. Le serveur recherche l'utilisateur global unique dont l'attribut de champ personnalisé #01 est égal à la valeur d'attribut Téléphone pour ce compte. Le nom que vous avez fourni pour l'attribut d'utilisateur global personnalisé à l'aide des propriétés globales de la tâche système n'est pas affiché ici. Si une correspondance unique est trouvée, le serveur de provisionnement associe le compte à l'utilisateur global. Si plusieurs correspondances sont trouvées, le serveur de provisionnement procède à l'étape 5. Si aucune correspondance n'est trouvée, le serveur de provisionnement procède à l'étape suivante.
5. Le serveur de provisionnement associe le compte avec l'objet [utilisateur par défaut]. Si l'objet [utilisateur par défaut] n'existe pas, le serveur le crée.

Ajout du terminal à l'environnement

Ajoutez le terminal à l'environnement sur lequel vous voulez le gérer. Un administrateur avec la tâche Créer un terminal peut effectuer cette procédure.

Procédez comme suit:

1. Sélectionnez Terminaux, Gérer les terminaux, Créer un terminal.
2. Sélectionnez un type de terminal.
3. Parcourez les onglets pour compléter les champs.

   Les champs obligatoires sont précédés d'un cercle rouge. Cliquez sur Aide pour accéder aux définitions des champs dans l'onglet actuel.

   Remarque : Evitez d'utiliser le symbole # dans le nom de terminal, car il n'est pas possible d'effectuer une recherche incluant ce caractère.
4. Cliquez sur Soumettre.

Vous êtes prêt à créer une Définition de corrélation et d'exploration (page 182) de façon à pouvoir gérer ses comptes.

Création d'une définition d'exploration et de corrélation

Pour ajouter des utilisateurs qui existent dans un terminal, créez une définition de corrélation et d'exploration pour ce terminal. Les administrateurs disposant de la tâche Créer une définition de corrélation et d'exploration peuvent créer la définition.

Procédez comme suit:

1. Dans un environnement, cliquez sur Terminaux, Définitions de corrélation et d'exploration, puis sur Créer une définition de corrélation et d'exploration.
2. Cliquez sur OK pour démarrer une nouvelle définition.
3. Renseignez un nom significatif de corrélation et d'exploration.
4. Cliquez sur Sélectionner un conteneur/un terminal/une méthode d'exploration pour choisir un terminal et des conteneurs, le cas échéant. Pour un grand terminal, la recherche de conteneur peut être longue ; vous pouvez utiliser le filtre de recherche pour affiner la recherche.
5. Cliquez sur une méthode d'exploration pour le conteneur. Le processus d'exploration et de corrélation inclut les conteneurs sélectionnés et les sous-conteneurs associés. Pour un conteneur d'annuaire, il inclut tous les conteneurs de la sous-arborescence.

6. Choisissez les actions de corrélation/d'exploration à effectuer.

   - **Explorer les objets gérés dans l'annuaire** : recherche les objets stockés sur le terminal et non dans l'annuaire de provisionnement.
   - **Etablir une corrélation entre les comptes et les utilisateurs** : établit une corrélation entre les objets trouvés dans la fonction d'exploration et les utilisateurs de l'annuaire de provisionnement. Il existe deux possibilités de corrélation.
     - **Utiliser l'utilisateur actuel**

       Utilisez cette option pour une règle de corrélation (page 179) qui correspond à chaque compte avec un utilisateur créé au préalable.

       Si l'utilisateur est trouvé, le compte est corrélé avec cet utilisateur. Si plusieurs utilisateurs sont trouvés, le compte est corrélé avec l'utilisateur par défaut. Si aucun utilisateur n'est trouvé, cette option crée l'utilisateur (si tous les attributs obligatoires sont connus) et corrèle le compte avec cet utilisateur ; dans le cas contraire, le compte est corrélé avec l'utilisateur par défaut.
     - **Créer des utilisateurs (si nécessaire)**

       Utilisez cette option lors de la corrélation de comptes sur votre terminal principal. Cette option suppose que les comptes sur votre terminal portent exactement le même nom que les utilisateurs. L'algorithme de correspondance de corrélation n'est pas utilisé avec cette option. Chaque compte est associé à l'utilisateur portant le même nom. Si l'utilisateur n'existe pas encore, il est créé. Aucun compte n'est associé à l'utilisateur par défaut.
   - **Mettre à jour les champs d'utilisateurs** : si un mappage existe entre les champs d'objets et les champs d'utilisateurs, ces derniers sont mis à jour avec les données provenant des champs d'objets.

     Les utilisateurs sont créés sans attributs facultatifs tels que le nom complet, l'adresse et les numéros de téléphone. Lors de l'acquisition initiale d'un terminal, utilisez cette option pour définir les attributs d'utilisateur grâce aux valeurs d'attribut de compte. Lors des explorations et corrélations suivantes, utilisez cette option pour actualiser les attributs d'utilisateur de manière à appliquer les modifications apportées aux attributs de compte, notamment par des outils autres que CA IdentityMinder.

7. Cliquez sur Soumettre.

Désormais, un administrateur avec la tâche Exécuter la corrélation et l'exploration (page 184) effectue l'intégration du terminal.

Exploration et corrélation d'un terminal

Un administrateur d'hébergement ou un autre administrateur disposant de la tâche Exécuter la corrélation et l'exploration suit cette procédure. La phase d'exploration de la tâche identifie les comptes dans le terminal. La phase de corrélation met en correspondance les comptes avec les utilisateurs dans CA IdentityMinder ou elle crée les comptes.

Procédez comme suit:

1. Dans un environnement, cliquez sur Terminaux, puis sur Exécuter la corrélation et l'exploration.
2. Sélectionnez Exécuter pour exécuter la corrélation et l'exploration immédiatement ou Planifier un nouveau job (page 366) pour exécuter la corrélation et l'exploration ultérieurement ou selon une planification récurrente.

   Remarque : Cette opération requiert que le navigateur du client et le serveur aient le même fuseau horaire. Par exemple, si l'heure du client est 22 h 00 le mardi et que l'heure du serveur est 07 h 00, la définition de corrélation et d'exploration ne fonctionne pas.
3. Cliquez sur une définition de corrélation et d'exploration à exécuter.
4. Cliquez sur Soumettre.

   Les comptes d'utilisateurs existant sur le terminal sont créés ou mis à jour dans CA IdentityMinder en fonction de la définition de corrélation et d'exploration que vous avez créée.
5. Vérifiez que la tâche est terminée en suivant cette procédure :
   a. Cliquez sur Système, Afficher les tâches soumises.
   b. Remplissez le champ avec le nom de tâche suivant : Exécuter la corrélation et l'exploration.
   c. Cliquez sur Rechercher.

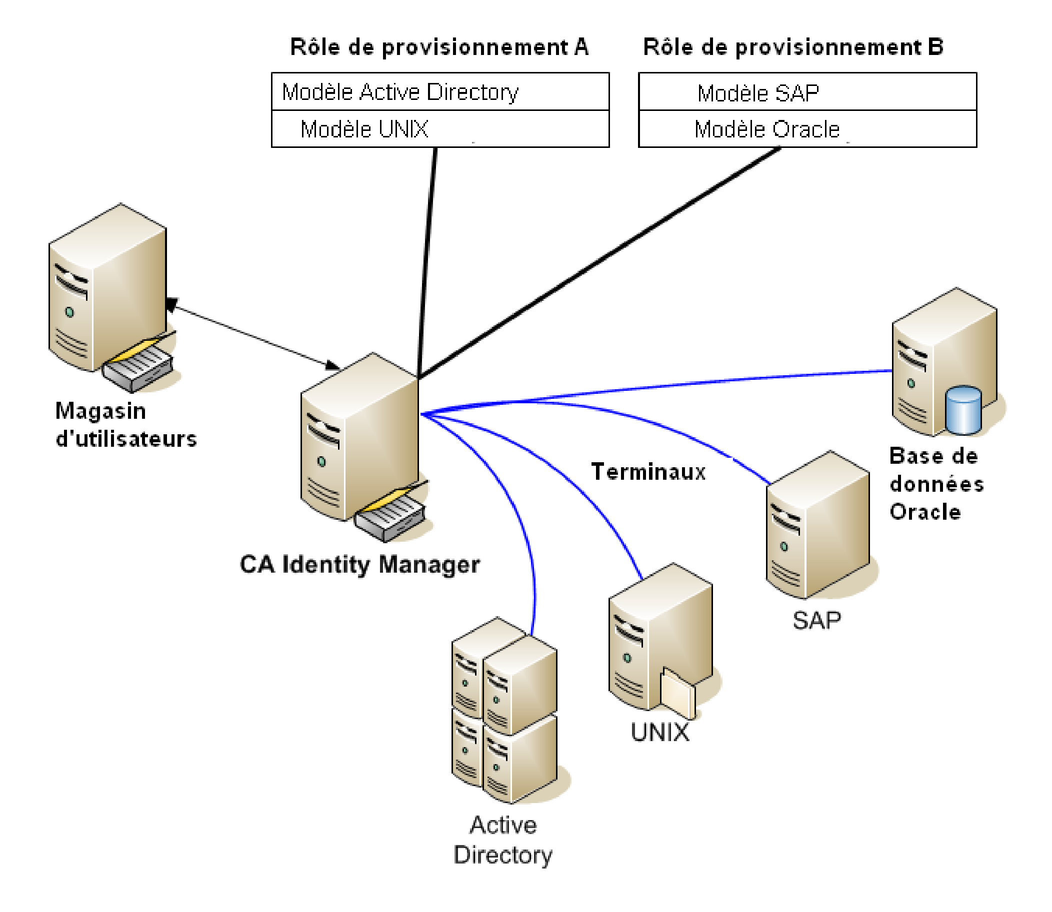
   Les résultats indiquent si la tâche s'est terminée correctement.

Remarque : Vous pouvez interrompre une tâche d'exploration et de corrélation lorsque vous affichez le statut de la tâche dans la section d'affichage des tâches soumises. L'interruption de la tâche empêche son traitement et la tâche affiche l'état en cours au moment de l'interruption. Toute notification générée est envoyée pour préserver la synchronisation des systèmes.

Synchronisation d'utilisateurs, de comptes et de rôles

L'intégration de plusieurs terminaux et comptes dans un système de gestion des utilisateurs unique peut entraîner une perte de synchronisation. Les rôles de provisionnement ou les modèles de compte qui sont affectés à un utilisateur peuvent différer des comptes réels qui existent pour cet utilisateur.

Par exemple, lorsque deux rôles de provisionnement sont utilisés, un avec des modèles de compte Active Directory et UNIX et l'autre avec des modèles SAP et Oracle. L'utilisateur john_smith dispose du rôle de provisionnement A qui contient les modèles de compte Active Directory et UNIX, mais il dispose uniquement d'un compte Active Directory. Il se peut que le modèle de compte UNIX ait été ajouté au rôle après son affectation à l'utilisateur. Par conséquent, l'administrateur synchronise l'utilisateur avec la définition de rôle actuelle.



Dans les cas suivants, une perte de synchronisation peut également se produire avec les rôles de provisionnement ou les modèles de compte :

- Les premières tentatives de création de comptes nécessaires ont échoué à cause de problèmes matériels ou logiciels dans votre réseau, entraînant la disparition de comptes.
- Modification des rôles de provisionnement et des modèles de compte, entraînant la création de comptes ou leur suppression.
- Les comptes ont été affectés aux modèles de comptes après leur création, les comptes existent donc, mais ils ne sont pas synchronisés avec leurs modèles de compte.
- La création d'un compte est retardée, car le compte a été défini pour être créé plus tard.
- Un nouveau terminal a été acquis. Lors de l'exploration et de la corrélation, le serveur de provisionnement n'a pas affecté de rôles de provisionnement aux utilisateurs automatiquement. Vous mettez à jour le rôle pour indiquer les utilisateurs qui requièrent des comptes sur le terminal. Un compte corrélé avec un utilisateur est répertorié comme compte supplémentaire lorsque l'utilisateur est synchronisé.
- Un compte existant a été affecté à un utilisateur en copiant le compte vers l'utilisateur.
- Un compte a été créé pour un utilisateur autrement qu'en affectant l'utilisateur à un rôle. Par exemple, vous avez copié un utilisateur dans un modèle de compte qui ne se trouve pas dans un rôle de provisionnement pour cet utilisateur. Le compte est répertorié comme un compte supplémentaire ou comme un compte avec un modèle de compte supplémentaire. Si vous copiez l'utilisateur vers un terminal pour créer un compte à l'aide du modèle de compte par défaut, ce compte peut être un compte supplémentaire.

Les sections suivantes décrivent les trois types de synchronisation :

1. Synchronisation d'utilisateurs avec des rôles (page 187)
2. Synchronisation d'utilisateur avec des modèles de compte (page 189)
3. Synchronisation de compte de terminal avec des modèles de compte (page 188)

Synchronisation d'utilisateurs avec des rôles

Cette tâche crée, met à jour ou supprime des comptes pour qu'ils soient conformes aux rôles de provisionnement affectés à un utilisateur. Par exemple, les administrateurs utilisent des outils natifs sur un terminal pour ajouter ou supprimer des comptes, mais vous n'avez pas réexploré ce terminal pour mettre à jour l'annuaire de provisionnement. Par conséquent, les utilisateurs peuvent constater des comptes supplémentaires ou manquants. Cette tâche assure également que chaque compte appartient aux modèles de compte corrects.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur.
2. Sélectionnez Utilisateurs, Synchronisation, Vérifier la synchronisation du rôle.
3. Sélectionnez un utilisateur.

   Une fenêtre s'affiche. Elle contient les comptes attendus, les comptes supplémentaires et les comptes manquants.
4. Cliquez sur Synchroniser pour procéder à la correspondance des comptes avec le modèle dans ce rôle.
   a. Vous pouvez sélectionner une case à cocher pour créer le compte sur le terminal. Si plusieurs modèles de compte pour l'utilisateur utilisent le même compte, le compte est créé en fusionnant tous les modèles de compte pertinents.

      Ce compte est affecté aux modèles de compte qui ne sont actuellement pas synchronisés avec le compte.
   b. Vous pouvez sélectionner une case à cocher pour supprimer les comptes supplémentaires. Toutefois, il se peut que les utilisateurs requièrent ces comptes. Si c'est le cas, n'activez pas cette option.

      Sur certains terminaux, la fonction de suppression de compte est désactivée ; par conséquent, le compte n'est pas supprimé.

Synchronisation d'utilisateur avec des modèles de compte

Cette tâche synchronise les attributs pour des comptes de terminal avec les modèles de compte associés pour un utilisateur. Toutefois, la synchronisation complète dépend de ces facteurs :

- La synchronisation complète du compte a lieu dans deux cas de figure. Un modèle de compte utilise la synchronisation forte (page 190) ou au moins deux modèles de compte ont été ajoutés à un compte.
- Si un modèle de compte utilise la synchronisation faible (page 190), cette tâche commence une synchronisation de compte impliquant uniquement ce modèle. Si le compte n'était pas préalablement inclus dans la synchronisation de compte avec d'autres modèles de compte avant cette mise à jour, il se peut qu'il ne soit toujours pas inclus dans la synchronisation de compte par la suite.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur.
2. Sélectionnez Utilisateurs, Synchronisation, Vérifier la synchronisation du modèle de compte.
3. Sélectionnez un utilisateur.

   Une fenêtre s'affiche. Elle contient les comptes attendus, les comptes supplémentaires et les comptes manquants.
4. Cliquez sur Synchroniser pour procéder à la correspondance des comptes avec le modèle.

   a. Vous pouvez sélectionner une case à cocher pour créer le compte sur le terminal. Si plusieurs modèles de compte pour l'utilisateur utilisent le même compte, le compte est créé en fusionnant les modèles de compte pertinents.

      Ce compte est affecté aux modèles qui ne sont pas synchronisés avec le compte. La synchronisation de compte n'est pas nécessaire pour les nouveaux comptes.

   b. Vous pouvez sélectionner une case à cocher pour supprimer les comptes supplémentaires. Toutefois, il se peut que les utilisateurs requièrent ces comptes. Si c'est le cas, n'activez pas cette option.

      Sur certains terminaux, la fonction de suppression de compte est désactivée ; par conséquent, le compte n'est pas supprimé.

Synchronisation des comptes de terminal avec les modèles de compte

Cette tâche synchronise un compte de terminal après la modification d'un modèle de compte associé. Par exemple, il se peut qu'un compte Active Directory n'inclue pas de groupes, mais que le modèle de compte associé soit défini pour inclure des groupes.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur.
2. Sélectionnez Terminaux, Gérer les terminaux, Vérifier la synchronisation des comptes de terminal.
3. Sélectionnez un terminal.

   Une fenêtre s'affiche. Elle contient les comptes de ce terminal, les modèles de compte associés et les attributs qui ne sont pas synchronisés.
4. Cliquez sur Synchroniser pour procéder à la mise en correspondance des attributs de ces comptes avec les valeurs définies dans le modèle de compte.

   Les modifications que vous apportez aux modèles de comptes affectent les comptes existants de la façon suivante :

   - Si vous modifiez la valeur d'un attribut de capacité, l'attribut de compte correspondant est mis à jour afin d'être synchronisé avec la valeur d'attribut de modèle de compte. Reportez-vous à la description des synchronisations faible et forte.
   - Certains attributs de compte sont conçus par le connecteur pour ne pas être mis à jour lors des modifications de modèle de compte. Par exemple, certains attributs que le type de terminal permet uniquement de définir pendant la création de compte et l'attribut Mot de passe.

Synchronisation des attributs de capacité

Lorsque vous modifiez les attributs de capacité d'un modèle de compte, l'attribut correspondant des comptes peut changer. L'impact sur les attributs d'un compte dépend de deux facteurs.

- Si le modèle de compte est défini pour utiliser une synchronisation faible ou forte
- Si le compte appartient à plusieurs modèles de compte

Synchronisation faible

La *synchronisation faible* garantit que les utilisateurs disposent des attributs de capacité minimum requis pour leurs comptes. La synchronisation faible est la valeur par défaut de la plupart des types de terminaux. Si vous mettez à jour un modèle qui utilise la synchronisation faible, CA IdentityMinder met à jour les attributs de capacité comme suit :

- Si un champ Numéro est mis à jour dans un modèle de compte et que le nouveau numéro est supérieur au numéro figurant dans le compte, CA IdentityMinder modifie la valeur du compte de manière à ce qu'elle corresponde au nouveau numéro.
- Si une case à cocher auparavant désactivée dans un modèle de compte est activée ultérieurement, CA IdentityMinder met à jour la case à cocher sur les comptes sur lesquels elle est désactivée.
- Si une liste est modifiée dans un modèle de compte, CA IdentityMinder met à jour tous les comptes pour inclure toutes les valeurs de la nouvelle liste qui n'étaient pas incluses dans la liste de valeurs du compte.

Si un compte appartient à d'autres modèles de compte (utilisant la synchronisation faible ou forte), CA IdentityMinder consulte uniquement le modèle en cours de modification. Cette action est plus efficace que la vérification de chaque modèle de compte. Dans la mesure où la synchronisation faible n'ajoute que des fonctionnalités aux comptes, il n'est généralement pas nécessaire de consulter ces autres modèles de compte.

Remarque : Lors de la propagation à partir d'un modèle de compte à synchronisation faible, il se peut que des modifications qui suppriment ou réduisent les fonctionnalités ne soient pas synchronisées vers certains comptes. N'oubliez pas que les fonctionnalités ne sont jamais supprimées ni réduites dans le cadre de la synchronisation faible. La propagation ne tient pas compte des autres modèles de comptes et des résultats de la synchronisation faible.

Dans cette situation, utilisez la synchronisation d'utilisateurs avec les modèles de compte pour synchroniser le compte avec ses modèles de compte.

Synchronisation forte

La synchronisation forte assure que les comptes incluent les mêmes attributs de compte que les attributs spécifiés dans le modèle de compte.

Par exemple, si vous ajoutez un groupe à un modèle de compte UNIX existant. Auparavant, le modèle de compte créait des membres de comptes du groupe Personnel. Désormais, vous voulez créer les membres de comptes des deux groupes Personnel et Système. Tous les comptes associés au modèle de compte sont synchronisés lorsque chaque compte devient membre des groupes Personnel et Système (et aucun autre groupe). Un compte n'appartenant pas au groupe Personnel est ajouté aux deux groupes.

Autres facteurs dont vous devez tenir compte :

- Si le modèle de compte utilise la synchronisation forte, les comptes appartenant à des groupes, autre que Personnel et Système, sont supprimés de ces autres groupes.
- Si le modèle de compte utilise la synchronisation faible, les comptes sont ajoutés aux groupes Personnel et Système. Les comptes pour lesquels d'autres groupes sont définis restent membres de ces groupes.

Remarque : Si vous n'appliquez pas les modifications aux comptes chaque fois que vous mettez à jour les attributs de capacité d'un modèle de compte, vous devez synchroniser régulièrement vos comptes avec leurs modèles de compte pour garantir la synchronisation des comptes avec leurs modèles.

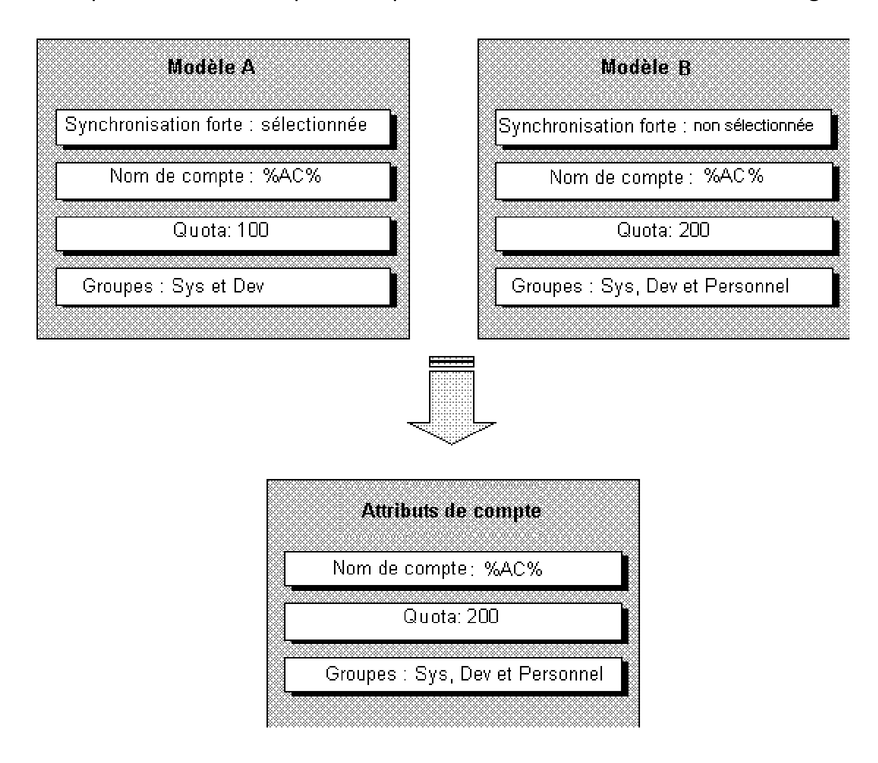
Comptes avec plusieurs modèles

La synchronisation dépend également de l'appartenance du compte à plusieurs modèles de compte. Si un compte inclut uniquement un modèle de compte et que ce modèle utilise la synchronisation forte, chaque attribut est mis à jour pour correspondre exactement à la valeur d'attribut du modèle de compte. Le résultat est le même qu'avec un attribut initial.

Un compte peut appartenir à plusieurs modèles de compte : c'est le cas lorsqu'un utilisateur global appartient à plusieurs rôles de provisionnement pour lesquels un même niveau d'accès est attribué sur le même terminal géré. Dans ce cas, CA IdentityMinder combine ces modèles de compte en un modèle de compte applicable qui attribut le sur-ensemble des fonctionnalités à partir des modèles de compte individuels. Ce modèle de compte utilise la synchronisation faible si tous ses modèles de compte individuels sont faibles ou la synchronisation forte si un des modèles de compte individuels est fort.

Remarque : Vous utilisez généralement uniquement la synchronisation faible ou uniquement la synchronisation forte pour les modèles de compte qui contrôlent un compte, si les rôles de votre société définissent intégralement les accès dont vos utilisateurs ont besoin. Si vos utilisateurs ne correspondent à aucun rôle clair et que vous ayez besoin de flexibilité pour attribuer des fonctionnalités supplémentaires aux comptes d'utilisateur, utilisez la synchronisation faible. Si vous êtes en mesure de définir des rôles pour spécifier exactement les accès dont vos utilisateurs ont besoin, utilisez la synchronisation forte.

L'exemple suivant décrit la combinaison de plusieurs modèles de compte en un modèle de compte unique applicable. Dans cet exemple, un modèle de compte est marqué pour la synchronisation faible et l'autre pour la synchronisation forte. Par conséquent, le modèle de compte applicable combinant les deux modèles de compte est considéré comme un modèle de compte de synchronisation forte. L'attribut Quota de nombre entier accepte la valeur la plus grande des deux modèles de compte et l'attribut Groupes à valeurs multiples accepte l'union des valeurs des deux stratégies.



Attributs uniquement pour les nouveaux comptes

Dans un modèle de compte, certains attributs sont uniquement appliqués lorsque vous créez un compte. Par exemple, l'attribut Mot de passe est un expression de règle qui définit le mot de passe pour les nouveaux comptes. Cette expression de règle ne met jamais à jour le mot de passe d'un compte. Les modifications apportées à l'expression de règle de mot de passe ont un impact uniquement sur les comptes créés après la définition de l'expression de règle.

De même, une expression de règle de modèle pour un attribut de compte en lecture seule affecte uniquement les comptes créés après la définition de l'expression de règle. Sa modification n'a aucun effet sur les comptes existants.

Synchronisation inversée avec des comptes de terminaux

Même si la création, la suppression et la modification de comptes incombe à CA IdentityMinder, il est impossible d'empêcher un utilisateur de système de terminal d'effectuer ces opérations lui-même. Cela peut se produire dans le cas de situations d'urgence ou de malveillance, comme dans le cas d'un pirate informatique. La synchronisation inversée garantit un contrôle des comptes qu'un utilisateur possède sur chaque terminal en identifiant les différences entre les comptes CA IdentityMinder et ceux sur les terminaux.

Par exemple, si un compte a été créé dans le domaine Active Directory à l'aide d'un outil externe, CA IdentityMinder doit être informé de ce problème de sécurité potentiel. En outre, le fait de contourner CA IdentityMinder entraîne un manque de processus d'approbation et de rapports d'audit.

Les deux types de différences entre CA IdentityMinder et les terminaux gérés sont les suivants.

- Détection d'un nouveau compte
- Modification d'un compte existant

Vous pouvez traiter ces deux cas en définissant des stratégies pour gérer le changement. Ensuite, en exécutant l'opération de corrélation et d'exploration pour mettre à jour CA IdentityMinder, vous déclenchez l'exécution des stratégies.

Fonctionnement de la synchronisation inversée

La synchronisation inversée avec des comptes de terminaux fonctionne comme suit.

1. Un administrateur ou un utilisateur malveillant crée ou modifie un compte sur un terminal.
2. Lorsque l'exploration et la corrélation s'exécutent sur ce terminal, le compte nouveau ou modifié est détecté.
3. Le serveur de provisionnement envoie une notification au serveur CA IdentityMinder.
4. Le serveur CA IdentityMinder recherche une stratégie de synchronisation inversée correspondant au changement opéré sur le terminal.
5. Si une stratégie correspondante est détectée, il l'exécute. Si plusieurs stratégies de même portée s'appliquent à ce compte, c'est la stratégie dont la priorité est la plus élevée qui s'exécute.
6. Selon la stratégie, l'une des actions suivantes est réalisée.
   - Pour un nouveau compte, la stratégie accepte, supprime ou suspend le compte ou l'envoie pour approbation du flux de travaux.
   - Pour un compte modifié, la stratégie accepte la valeur, rétablit la dernière valeur connue ou envoie la modification pour approbation du flux de travaux.
7. Si un flux de travaux est sélectionné, un nouvel événement est généré pour celui-ci et les approbateurs sont définis. Ensuite, l'une des actions suivantes est réalisée.
   - Pour un nouveau compte, l'approbateur peut accepter, supprimer ou suspendre le compte, ou encore l'affecter à un utilisateur.
   - Pour un compte modifié, le processus de flux de travaux est le même que si la valeur avait été modifiée dans la console d'utilisateur, si ce n'est que les valeurs rejetées sont inversées au niveau du terminal.

Mappage d'attributs de terminal

Chaque attribut d'un compte de terminal que vous souhaitez gérer avec une synchronisation inversée doit être mappé vers un attribut d'utilisateur global. La plupart des attributs de profil d'utilisateur initiaux, comme le nom de compte, le mot de passe et l'état du compte, sont mappés par défaut. D'autres attributs ne le sont toutefois pas, par exemple, les attributs de capacité.

Pour mapper des attributs de terminal pour la synchronisation inversée

1. Dans la console d'utilisateur, procédez comme suit.
    a. Cliquez sur Terminaux, Modifier le terminal.
    b. Recherchez et sélectionnez un terminal qui nécessite une synchronisation inversée.
    c. Cliquez sur l'onglet Mappage d'attributs.
    d. Cochez Utiliser les paramètres personnalisés.
    e. Cliquez sur Set Default (Définir les valeurs par défaut) pour restaurer les paramètres par défaut dans la liste.
    f. Cliquez sur Ajouter pour insérer un nouvel attribut personnalisé.
    g. Sélectionnez un attribut personnalisé disponible. Vous pouvez, par exemple, utiliser CustomField 10 s'il n'est pas mappé pour utilisation dans votre environnement.
    h. Mappez l'attribut personnalisé vers le nom de l'attribut de compte à gérer.
    i. Cliquez sur OK.
    j. Répétez les étapes f à i pour ajouter des mappages entre tous les attributs de compte nécessaires et l'attribut personnalisé sélectionné.

       Vous pouvez utiliser le même attribut personnalisé (CustomField 10 dans notre exemple) pour tous les attributs à gérer.
    k. Cliquez sur OK.
2. Dans le gestionnaire de provisionnement, désactivez la notification entrante de la manière suivante.
    a. Cliquez sur System (Système), Domain configuration (Configuration de domaine), CA IdentityMinder Server, Enable Notification (Autoriser la notification).
    b. Sélectionnez Non.
    c. Redémarrez le serveur de provisionnement pour vous assurer de la prise d'effet du changement.

   Important : La désactivation de la notification entrante élimine les notifications superflues pendant l'opération d'exploration et de corrélation. Sinon, chaque compte qui possède des valeurs sur les nouveaux attributs génère une notification.

3. Dans la console d'utilisateur, cliquez sur Terminaux, puis sur Exécuter la corrélation et l'exploration.
4. Sélectionnez une définition de corrélation et d'exploration dont la corrélation est désélectionnée.

   Cette action renseigne les attributs de magasin d'utilisateurs avec les nouvelles données d'attribut de terminal. Cette tâche peut prendre un certain temps si le terminal est volumineux.
5. Réactivez la notification entrante dans le gestionnaire de provisionnement.

Lors de la prochaine exécution de corrélation et d'exploration pour ce terminal, des notifications de modification de compte sont générées. Des notifications sont générées en cas de modification d'un attribut qui est mappé vers un attribut d'utilisateur global et auquel une stratégie s'applique.

Informations complémentaires :

Attributs de capacité et initiaux (page 226)

Stratégies pour la synchronisation inversée

Lorsqu'un compte est créé ou modifié sur un terminal, les stratégies de synchronisation inversée peuvent prendre des mesures appropriées en retour. Imaginons, par exemple, qu'un utilisateur crée des comptes Active Directory dans plusieurs unités organisationnelles du domaine d'entreprise. Il modifie aussi des comptes Microsoft Exchange. Vous pouvez détecter les comptes nouveaux et modifiés et prendre des mesures adéquates en retour en utilisant des stratégies de synchronisation inversée.

La synchronisation inversée vous permet d'effectuer les opérations suivantes.

- Configurer une stratégie pour accepter le nouveau compte, le rejeter ou l'envoyer pour approbation du flux de travaux.
- Configurer une stratégie pour accepter une modification apportée à un attribut, la rejeter afin de revenir à l'attribut initial ou l'envoyer pour approbation du flux de travaux.
- Lorsqu'un compte est envoyé pour approbation du flux de travaux, l'approbateur peut exécuter l'une des actions suivantes.
  - Le rejeter (le supprimer/le suspendre du terminal ou modifier la valeur pour la faire correspondre à la valeur du magasin d'utilisateurs CA IdentityMinder).
  - L'accepter et mettre à jour le magasin d'utilisateurs CA IdentityMinder pour qu'il corresponde au compte.
  - L'affecter à un utilisateur dans la console d'utilisateur (en cas de création d'un compte).

Création d'une stratégie pour de nouveaux comptes

Si vous souhaitez définir un processus pour les cas où un nouveau compte est détecté sur un terminal, créez une stratégie de compte qui s'applique aux nouveaux comptes. Les stratégies de nouveaux comptes s'exécutent à la détection de comptes lorsque l'option de corrélation est incluse dans la définition de corrélation et d'exploration. Si un compte a été détecté lors de l'exécution de l'exploration uniquement, la stratégie s'exécute la prochaine fois que l'option de corrélation est incluse lors de l'exploration de ce terminal.

Pour créer une stratégie pour de nouveaux comptes

1. Dans la console d'utilisateur, cliquez sur Terminaux, Inverser la création, Créer une stratégie de nouveau compte via la synchronisation inversée.
2. Entrez un nom et une description pour la stratégie.
3. Entrez les paramètres suivants.
   - Priorité : priorité de la stratégie. La stratégie dont la priorité est la plus élevée est celle dont le nombre est le plus petit. Si deux stratégies présentent la même priorité et la même portée, l'une ou l'autre stratégie peut s'exécuter. Veillez donc à définir des niveaux de priorité différents.
   - Type de terminal : tous les terminaux ou un type de terminal spécifique.
   - Terminal : nom de terminal spécifique. Si Type de terminal est défini sur Tout, le seul choix possible est Tous les terminaux.
   - Conteneur : conteneur où réside le compte. Ce champ s'applique uniquement aux terminaux hiérarchiques. Entrez le conteneur en tant que liste de noeuds, en finissant par le terminal. Par exemple, pour une unité organisationnelle Active Directory avec le chemin "ou=enfant,ou=parent,ou=racine,dc=domaine,dc=nom", le format "enfant,parent,racine" est correct.
   - Utilisateur en corrélation : contrôle à quel moment exécuter la stratégie en fonction de la détection d'un utilisateur en corrélation dans l'annuaire de provisionnement.

4. Sélectionnez l'une des actions suivantes.
   - Accepter : n'entreprend aucune action sur le compte. Ce choix est utile si deux stratégies coexistent, une qui rejette tous les nouveaux comptes et une autre de priorité supérieure qui accepte les comptes créés sous une certaine unité organisationnelle. Par conséquent, si le compte a été créé sous cette unité organisationnelle, il est accepté. La priorité de rejet n'est pas exécutée vu qu'elle est plus faible.
   - Supprimer : supprime le compte du terminal.
   - Suspendre : laisse le compte sur le terminal, mais le suspend.
   - Envoi pour approbation : envoie la modification pour approbation du flux de travaux.
5. Si vous définissez l'action sur Envoi pour approbation, effectuez les opérations suivantes.
   a. Cliquez sur l'icône en regard de Processus de flux de travaux.
   b. Choisissez un processus de flux de travaux.
   c. Cliquez sur OK.
6. Cliquez sur Soumettre.

Si vous avez affecté un processus de flux de travaux à la stratégie, vous devez créer une tâche d'approbation (page 201).

Création d'une stratégie pour des comptes modifiés

N'importe quel attribut d'un compte de terminal peut être géré par la synchronisation inversée, pour autant qu'il soit défini dans le mappage d'attributs (page 195).

Pour définir un processus pour les cas où une incohérence est détectée entre des comptes de terminaux existants et leurs valeurs connues dans CA IdentityMinder, vous pouvez créer une stratégie de compte qui s'applique aux comptes existants. Si un attribut est à valeurs multiples, il est possible que plusieurs valeurs aient été ajoutées ou supprimées. Dans ce cas, la stratégie est appliquée à chaque valeur séparément ou vous pouvez également créer des stratégies distinctes pour différentes valeurs.

Pour créer une stratégie pour des comptes modifiés

1. Dans la console d'utilisateur, cliquez sur Terminaux, Inverser la modification, Créer une stratégie de compte modifié via la synchronisation inversée.
2. Entrez un nom et une description pour la stratégie.
3. Entrez les paramètres suivants.
   - Priorité : priorité de la stratégie. La stratégie dont la priorité est la plus élevée est celle dont le nombre est le plus petit. Si deux stratégies présentent la même priorité et la même portée, l'une ou l'autre stratégie peut s'exécuter. Veillez donc à définir des niveaux de priorité différents.
   - Type de terminal : tous les terminaux ou un type de terminal spécifique.
   - Terminal : nom de terminal spécifique. Si Type de terminal est défini sur Tout, le seul choix possible est Tous les terminaux.
   - Conteneur : conteneur où réside le compte. Ce champ s'applique uniquement aux terminaux hiérarchiques. Entrez le conteneur en tant que liste de noeuds, en finissant par le terminal. Par exemple, pour une unité organisationnelle Active Directory avec le chemin "ou=enfant,ou=parent,ou=racine,dc=domaine,dc=nom", le format "enfant,parent,racine" est correct.
   - Attribut : nom physique.
   - Valeur : représentation de la valeur sous forme de chaîne pouvant contenir le caractère générique ***** (astérisque). Ce caractère générique se rapporte à toute valeur de la modification.

4. Sélectionnez l'une des actions suivantes.
   - Accepter : met à jour la valeur du compte dans le magasin d'utilisateurs CA IdentityMinder pour la faire correspondre à celle du compte du terminal.
   - Rejeter : rétablit la valeur originale de l'attribut sans impliquer d'autres modifications pour les attributs du compte.
   - Envoi pour approbation : envoie la modification pour approbation du flux de travaux.
5. Si vous définissez l'action sur Envoi pour approbation, effectuez les opérations suivantes.
   a. Cliquez sur l'icône en regard de Processus de flux de travaux.
   b. Choisissez un processus de flux de travaux.
   c. Cliquez sur OK.
6. Cliquez sur Soumettre.

Si vous avez affecté un processus de flux de travaux à la stratégie, vous devez créer une tâche d'approbation (page 201).

Création d'une tâche d'approbation pour la synchronisation inversée

Vous créez des tâches d'inversion d'approbation pour les stratégies intégrant une action d'envoi au flux de travaux. Pour la création des tâches, tenez compte des directives ci-dessous.

- Pour les tâches qui approuvent de nouveaux comptes, vous avez deux possibilités.
  - Vous pouvez créer une fenêtre d'approbation générique pour les comptes. La fenêtre de profil de la tâche n'affiche que des informations générales sur le compte. La tâche Approuver l'inversion du nouveau compte fonctionne de cette manière.
  - Si l'approbateur doit consulter les détails du nouveau compte, cette fenêtre doit être spécifique au type de terminal. Par conséquent, la tâche d'approbation avec la fenêtre ne doit être utilisée que pour les stratégies spécifiques à ce type de terminal. La tâche doit inclure l'onglet Inverser l'approbation.
- Pour les tâches qui approuvent des modifications de compte, la fenêtre d'approbation doit être spécifique à un type de terminal, de sorte que l'approbateur puisse consulter les valeurs modifiées.

Les tâches d'inversion d'approbation sont identiques aux tâches d'approbation utilisées pour les modifications de compte. Si une tâche d'approbation pour un type de terminal spécifique existe déjà, vous pouvez l'utiliser. Pour un nouveau compte, un autre onglet Inverser l'approbation est nécessaire. S'il n'existe pas de tâche d'approbation pour le type de terminal, procédez comme suit.

Pour créer une tâche d'approbation pour la synchronisation inversée

1. Dans la console d'utilisateur, cliquez sur Rôles et tâches, Tâches d'administration, Créer une tâche d'administration.
2. Sélectionnez la tâche de modification pour le terminal.

   Son nom doit commencer par "modifier" et indiquer le nom du type de terminal. Par exemple, Modifier le compte Active Directory.
3. Apportez les modifications suivantes sous l'onglet Profil.
   - Renommez la nouvelle tâche.
   - Modifiez la balise de la tâche.
   - Remplacez l'action par Approuver un événement.
4. Apportez les modifications suivantes sous l'onglet Onglets.
   a. Supprimez tous les onglets Relation.
   b. Ajoutez l'onglet Inverser l'approbation si la tâche doit approuver de nouveaux comptes. Déplacez cet onglet pour qu'il soit le premier.
5. Cliquez sur Soumettre.

6. Si la tâche concerne des approbations de nouveaux comptes, ajoutez la tâche à un rôle auquel l'approbateur appartient. Le rôle définit la portée de l'utilisateur qui est utilisée pour rechercher des utilisateurs auxquels le nouveau compte peut être affecté.

Exécution de la synchronisation inversée

La synchronisation inversée s'exécute lorsque vous utilisez la tâche Exécuter la corrélation et l'exploration. Cette tâche vous permet de mettre à jour le magasin d'utilisateurs CA IdentityMinder en fonction des comptes nouveaux ou modifiés sur un terminal.

Pour exécuter la synchronisation inversée

1. Créez une définition de corrélation et d'exploration qui inclut une option de corrélation. La corrélation est nécessaire pour détecter de nouveaux comptes.
2. Cliquez sur Terminaux, Exécuter la corrélation et l'exploration
3. Choisissez une définition qui s'applique au terminal incluant les comptes nouveaux ou modifiés.

   Remarque : Lors de la corrélation avec l'utilisateur existant, l'utilisateur doit exister dans l'annuaire de provisionnement, sinon l'utilisateur est corrélé avec l'utilisateur par défaut de cet annuaire. Le magasin d'utilisateurs CA IdentityMinder n'est pas dans la portée de la tâche d'exploration et de corrélation.
4. Cliquez sur Soumettre.

Si une stratégie ne contient pas de processus de flux de travaux, les comptes sont déjà traités comme définis dans la stratégie. Si plusieurs attributs ont été rejetés sur un compte détecté par une stratégie de synchronisation inversée, toutes les actions sont rassemblées en un seul événement. Toutefois, si cet événement échoue en raison d'un problème lié à un des attributs, aucun de ceux-ci n'est mis à jour.

Si le flux de travaux fait partie de la stratégie, toutes les approbations générées par la synchronisation inversée apparaissent sous Flux de travaux, Afficher ma liste de travail pour l'approbateur.

Pour les nouveaux comptes, l'approbateur peut opérer les choix suivants.

- L'approbateur peut choisir de suspendre ou de supprimer le compte dans le terminal, en sélectionnant Supprimer ou Suspendre puis en cliquant sur Rejeter.
- Il peut également accepter le nouveau compte en cliquant sur Approuver.

  Si l'approbateur ne sélectionne pas un utilisateur dans le champ Utilisateur en corrélation, le compte est affecté à l'utilisateur par défaut. Si le champ Utilisateur en corrélation est renseigné dans la tâche d'approbation, le compte est corrélé avec cet utilisateur. Le champ Utilisateur en corrélation contient l'utilisateur suggéré détecté par le mécanisme de corrélation le cas échéant.

Pour les comptes modifiés, l'approbateur peut opérer les choix suivants.

- Pour chaque compte, l'approbateur voit les valeurs modifiées et peut les approuver ou les rejeter comme si les changements avaient été initiés dans les fenêtres de gestion des comptes.

- L'approbateur voit les changements apportés aux attributs de capacité (par exemple, des groupes Active Directory) comme des événements d'approbation distincts.

Pour vérifier si la synchronisation inversée a réussi

1. Accédez à Système, Afficher les tâches soumises.
2. Renseignez "Activité de provisionnement" dans le champ Nom de la tâche.
3. Cliquez sur Rechercher.

Les résultats s'affichent si les événements de synchronisation inversée se sont terminés correctement.

Extension des attributs personnalisés sur les terminaux

Le serveur de provisionnement peut gérer les attributs de terminal personnalisés. Des étapes supplémentaires sont requises pour permettre à CA IdentityMinder de lire les attributs de terminal personnalisés associés aux rôles de provisionnement.

Pour étendre les attributs personnalisés sur les terminaux :

1. Générez les métadonnées à partir de la table de l'analyseur si ce connecteur a été créé avant CA IdentityMinder r12.5.

   Reportez-vous au *manuel de programmation de Java Connector Server* (en anglais).

2. Utilisez Connector Xpress comme suit.

   a. Installez les métadonnées dans le noeud de l'espace de noms.

   b. Générez un fichier JAR, un fichier de propriétés et un fichier de définitions de rôles à l'aide du générateur de définitions de rôles.

      Pour plus d'informations, reportez-vous au *guide de Connector Xpress* (en anglais).

3. Copiez le fichier JAR à l'emplacement suivant.

   ■ (Windows) *répertoire d'installation du serveur d'applications*/iam_im.ear/user_console.war/WEB-INF/lib

   ■ (UNIX) *répertoire d'installation du serveur d'applications*\iam_im.ear\user_console.war\WEB-INF\lib

   Remarque : Pour WebSphere, copiez le fichier JAR à l'emplacement suivant : WebSphere_home/AppServer/profiles/*Nom_profil*/config/cells/*Nom_cellule*/applications/iam_im.ear/user_console.war/WEB-INF

4. Copiez le fichier JAR à l'emplacement suivant.

   ■ (Windows) *répertoire d'installation du serveur d'applications*/iam_im.ear/custom/provisioning/resourceBundles

   ■ (UNIX) *répertoire d'installation du serveur d'applications*\iam_im.ear\custom\provisioning\resourceBundles

   Remarque : Pour WebSphere, copiez le fichier de propriétés à l'emplacement suivant :

   WebSphere_home/AppServer/profiles/*Nom_profil*/config/cells/*Nom_cellule*/applications/iam_im.ear\custom\provisioning\resourceBundles

5. Répétez les deux étapes précédentes pour chaque noeud si vous disposez d'un cluster.

6. Redémarrez le serveur d'applications.

7. Importez le fichier de définitions de rôles comme suit :

   a. Dans la console de gestion, sélectionnez l'environnement.

   b. Sélectionnez les paramètres de tâches et de rôles.

   c. Cliquez sur Importer.

   d. Sélectionnez le type de terminal, puis cliquez sur Terminer.

Tâches associées aux comptes

Dans la console d'utilisateur, vous pouvez créer, modifier, afficher et supprimer les comptes de terminal associés à un utilisateur Identity Manager. Vous pouvez également affecter d'autres comptes de terminaux non associés à CA IdentityMinder à un utilisateur.

Il existe quatre types de comptes de terminaux.

Provisionné

Comptes créés lorsqu'un rôle de provisionnement est affecté à l'utilisateur

Exception

Comptes créés lorsqu'un modèle de compte est affecté à l'utilisateur

Orphelin

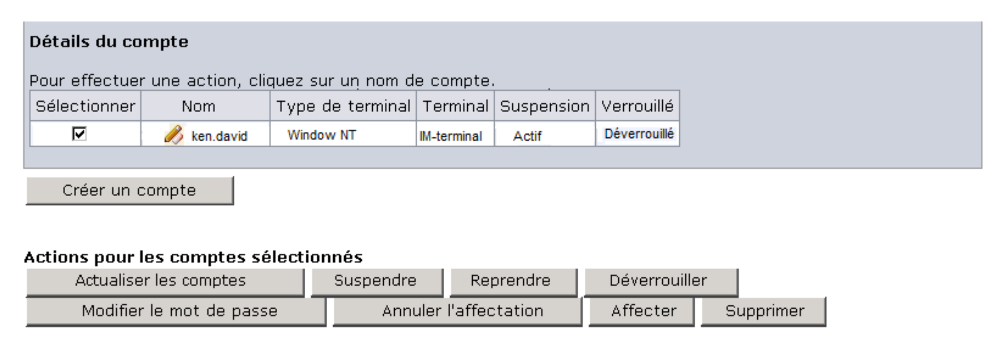
Comptes créés sur le terminal, non associés à un utilisateur CA IdentityMinder

Système

Comptes créés sur le terminal, non associés à un utilisateur CA IdentityMinder et permettant de gérer le terminal

Affichage ou modification de comptes de terminal

Les tâches permettant d'afficher le profil d'un utilisateur, telles que Afficher l'utilisateur ou Modifier mon profil, incluent un onglet Comptes qui répertorie les comptes de cet utilisateur sur les terminaux.



Pour chaque compte, Identity Manager affiche les informations telles que le nom du compte, le terminal du compte et le statut du compte. Pour une tâche Modifier, les options supplémentaires sont disponibles pour changer le mot de passe d'un utilisateur et verrouiller ou suspendre un compte.

Dans cet exemple, l'onglet Comptes inclut un bouton Rechercher, indiquant que l'onglet est configuré avec une fenêtre de recherche. Vous pouvez configurer cet onglet pour utiliser une fenêtre de liste, une fenêtre de recherche, ou les deux.

- Lorsque les deux fenêtres sont configurées, la fenêtre de recherche détermine les champs dans les résultats de la recherche.
- Si uniquement la fenêtre de liste est configurée, elle détermine les champs dans les résultats de la recherche.
- Si aucune des deux fenêtres n'est configurée, l'onglet de comptes utilise un affichage de liste statique, ce qui signifie que l'affichage des colonnes ne peut pas être personnalisé dans l'onglet Comptes.

Pour obtenir des détails sur les autres options pouvant être définies dans l'onglet Comptes, consultez dans l'aide de la console d'utilisateur la section sur l'onglet de configuration de comptes.

Création d'un compte provisionné

La méthode recommandée de création d'un compte de terminal pour un utilisateur CA IdentityMinder consiste à affecter un rôle de provisionnement à l'utilisateur. L'utilisateur reçoit le compte avec les attributs définis dans les modèles de compte de ce rôle. Le cas échéant, les modifications apportées au modèle de compte, telles que la taille de boîte aux lettres des comptes Exchange, mettent à jour le compte de terminal.

Pour créer un compte provisionné :

1. Dans la console d'utilisateur, sélectionnez Gérer les utilisateurs, puis Modifier l'utilisateur.
2. Sélectionnez l'utilisateur à modifier.
3. Cliquez sur l'onglet Rôles de provisionnement.
4. Cliquez sur Ajouter un rôle de provisionnement.
5. Sélectionnez un rôle.
6. Cliquez sur Soumettre.

Création d'un compte d'exception

Vous pouvez créer un compte directement dans l'onglet Comptes lorsque vous utilisez la tâche Modifier l'utilisateur sur un utilisateur. Ce compte est appelé compte d'exception. Aucun rôle de provisionnement n'étant lié à ce type de compte, la synchronisation des rôles avec les utilisateurs ne met pas ce compte à jour.

Pour créer un compte d'exception :

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, puis Modifier les comptes de terminaux de l'utilisateur.
2. Sélectionnez l'utilisateur à modifier.
3. Cliquez sur Créer.
4. Sélectionnez un terminal.
5. Sélectionnez un conteneur si ce type de terminal en requiert un.
6. Complétez les champs des onglets.
7. Cliquez sur Soumettre.

Affectation de comptes orphelins

Dans la console d'utilisateur, vous pouvez gérer les comptes orphelins. Ceux-ci ne sont associés à aucun utilisateur CA IdentityMinder.

Pour créer un utilisateur par défaut pour les comptes orphelins :

Si l'annuaire de provisionnement est différent du magasin d'utilisateurs CA IdentityMinder, créez l'utilisateur par défaut du serveur de provisionnement dans le magasin d'utilisateurs CA IdentityMinder. L'utilisateur par défaut est utilisé pour les comptes orphelins.

1. Dans la console d'utilisateur, cliquez sur l'onglet Utilisateurs.
2. Cliquez sur Gérer les utilisateurs, Créer un utilisateur.
3. Renommez l'utilisateur comme suit (crochets inclus).
   `[utilisateur par défaut]`

   Vous pouvez à présent affecter des comptes orphelins aux utilisateurs.

Pour affecter un compte orphelin :

1. Dans la console d'utilisateur, cliquez sur Terminaux.
2. Cliquez sur Gérer les comptes orphelins.
3. Recherchez et sélectionnez un utilisateur.
4. Cliquez sur un utilisateur à affecter au compte orphelin.

Affectation de comptes système

Dans la console d'utilisateur, vous pouvez gérer des comptes système, qui sont des comptes de terminal utilisés pour gérer le système d'extrémité.

Pour affecter un compte système à un utilisateur, créez une tâche d'administration basée sur la tâche Gérer les comptes système. La nouvelle tâche est associée à un utilisateur CA IdentityMinder spécifique qui postule à un terminal donné. Vous pouvez créer une tâche pour chaque type de terminal.

Pour configurer une tâche d'affectation de comptes système :

1. Dans la console d'utilisateur, cliquez sur Rôles et tâches, Tâches d'administration, puis Créer une tâche d'administration.
2. Basez la nouvelle tâche sur l'option Gérer les comptes système.

   Par exemple, vous pouvez créer une tâche nommée *Gérer les comptes système Oracle* pour affecter des comptes système sur un type de terminal Oracle.

3. Dans l'onglet Rechercher, cliquez sur le bouton Parcourir pour modifier la fenêtre de recherche. Dans cette même fenêtre, incluez un filtre de recherche sur un utilisateur à affecter à ce compte système .
4. Soumettez la tâche.
5. Incluez cette tâche dans un rôle.
6. Affectez le rôle à un utilisateur chargé d'affecter les comptes système d'un terminal à un autre utilisateur.

   L'utilisateur avec ce rôle peut exécuter la nouvelle tâche pour affecter des comptes système à un utilisateur CA IdentityMinder.

Fenêtre de tâche Déplacer un compte

Cette fenêtre de tâche permet de déplacer des comptes d'un conteneur d'un terminal à un autre. Les champs qu'elle contient sont répertoriés ci-dessous.

Déplacer les détails du compte

Spécifie le compte, le conteneur parent, le conteneur de destination, le terminal et le type de terminal à déplacer.

Bouton Sélectionner un conteneur

Cliquez sur ce bouton pour rechercher des conteneurs de compte disponibles appartenant au terminal.

Suppression d'un compte de terminal

Pour supprimer un compte de terminal, procédez de l'une des façons suivantes.

1. A l'aide de la tâche Modifier l'utilisateur, dans l'onglet Rôles de provisionnement, supprimez le rôle à l'origine de la création du compte.
2. A l'aide de la tâche Modifier les comptes de terminaux de l'utilisateur, supprimez le compte.

Pour supprimer un compte à l'aide de la tâche Modifier les comptes de terminaux de l'utilisateur :

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, puis Modifier les comptes de terminaux de l'utilisateur.
2. Sélectionnez l'utilisateur à modifier.
3. Recherchez les comptes basés sur un type de terminal.
4. Sélectionnez un compte.
5. Cliquez sur le bouton Supprimer.

Les comptes supprimés sont recréés lorsque vous utilisez le gestionnaire de provisionnement comme suit :

- L'opération Synchroniser l'utilisateur avec les rôles permet de recréer les comptes provisionnés (comptes créés lorsqu'un utilisateur a un rôle de provisionnement).
- L'opération Synchroniser les comptes avec les modèles de compte permet de recréer les comptes d'exception (si le compte dispose d'un modèle de compte) et les comptes provisionnés.

Modification du mot de passe d'un compte de terminal

Vous pouvez modifier le mot de passe d'un compte de terminal sans connaître le mot de passe actuel.

Pour modifier le mot de passe d'un compte de terminal :

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, puis Modifier les comptes de terminaux de l'utilisateur.
2. Sélectionnez l'utilisateur à modifier.
3. Recherchez les comptes basés sur un type de terminal.
4. Sélectionnez un ou plusieurs comptes.

5. Cliquez sur le bouton Modifier le mot de passe.
6. Entrez un nouveau mot de passe.

   Les stratégies de mot de passe de CA IdentityMinder valident le nouveau mot de passe.
7. Cliquez sur Soumettre.

Exécution d'actions sur plusieurs comptes

Vous pouvez effectuer plusieurs autres actions sur un ou plusieurs comptes. Par exemple, vous pouvez reprendre un compte suspendu, déverrouiller un compte suite à la saisie d'un mot de passe incorrect par l'utilisateur ou affecter/annuler l'affectation d'un compte à un utilisateur. Les actions s'appliquent à tous les comptes sélectionnés et la procédure est identique.

Pour effectuer des tâches sur plusieurs comptes :

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, puis Modifier les comptes de terminaux de l'utilisateur.
2. Sélectionnez l'utilisateur à modifier.
3. Recherchez les comptes basés sur un type de terminal.
4. Sélectionnez un ou plusieurs comptes.
5. Cliquez sur un des boutons sous Actions pour les comptes sélectionnés.
6. Répondez à la boîte de dialogue qui s'affiche, puis cliquez sur Soumettre.

Opérations avancées de compte

Le gestionnaire de provisionnement permet d'effectuer de nombreuses opérations supplémentaires sur des comptes :

- Association d'un compte à différents utilisateurs globaux
- Exploration automatique de comptes
- Suppression de comptes
- Utilisation de la suppression en attente
- Recréation de comptes supprimés

Modification de l'utilisateur global d'un compte

Voici différentes situations lors desquelles vous voudrez probablement associer un compte à un utilisateur global différent :

- Deux utilisateurs globaux portent le même nom et CA IdentityMinder corrèle le compte avec l'utilisateur incorrect.
- CA IdentityMinder a corrélé un compte à l'objet [utilisateur_par_défaut] et vous souhaitez l'associer à un autre objet d'utilisateur global.
- Vous avez créé un compte à l'aide de l'option Créer et vous souhaitez désormais l'associer à un utilisateur global.

Pour associer un compte à un utilisateur global différent dans le gestionnaire de provisionnement, utilisez la fonction glisser-déposer et déplacez le compte vers l'utilisateur global correct.

Fonctionnement de l'exploration automatique

CA IdentityMinder ne perçoit pas l'ajout ou la suppression de comptes ou d'autres objets à l'aide d'outils natifs dans le terminal, jusqu'à l'exploration de ce dernier. Le processus d'exploration décèle les ajouts et les suppressions (et dans certains cas, les modifications) survenus et les applique à la représentation CA IdentityMinder de l'objet dans l'annuaire de provisionnement.

Toutefois, si vous tentez de créer un objet portant le même nom à l'aide du gestionnaire de provisionnement avant cette exploration, CA IdentityMinder note qu'un objet portant ce nom existe déjà et signale cette erreur. CA IdentityMinder explorera ensuite cet objet et en créera une représentation dans l'annuaire de provisionnement. Vous pouvez commencer immédiatement à utiliser cet objet. L'exploration automatique d'un objet survient lorsqu'une opération d'ajout, de déplacement ou de modification de nom génère une erreur signalant un objet existant à partir du terminal lorsque l'objet n'existe pas dans l'annuaire de provisionnement.

Vous pouvez combiner l'exploration automatique avec le paramètre de configuration du domaine de synchronisation/corrélation automatique décrit dans le Manuel *Provisioning Reference Guide (Manuel de référence du provisionnement)*. Lorsque ces fonctionnalités interagissent, elles traitent d'abord une tentative de création d'un compte à partir d'un modèle de compte comme une tentative de création de compte classique. Puis, le traitement suit la procédure suivante :

- Découverte d'un compte inexploré
- Exploration automatique de ce compte
- Corrélation automatique du compte avec l'utilisateur global
- Ajout d'un modèle de compte au compte comme dans le cas d'un compte existant corrélé avec cet utilisateur global

Suppression de comptes

Si vous devez supprimer un compte, vous pouvez appliquer les méthodes suivantes dans le gestionnaire de provisionnement :

- Cliquez avec le bouton droit de la souris sur le compte et sélectionnez Supprimer.
- Cliquez avec le bouton droit de la souris sur un utilisateur global et sélectionnez Supprimer des comptes.
- Exécutez l'assistant Supprimer des comptes.
- Synchronisez des utilisateurs globaux avec des rôles de provisionnement et spécifiez que vous voulez supprimer d'autres comptes.

Lorsque vous supprimez un utilisateur global d'un rôle de provisionnement, le gestionnaire de provisionnement fournit les choix suivants pour la suppression de comptes :

- Si vous décidez de supprimer ces comptes, CA IdentityMinder les supprimera de l'annuaire de provisionnement.
- Sinon, vous pouvez utiliser l'option Synchroniser l'utilisateur avec des rôles et sélectionnez Supprimer un compte.

Si vous supprimez un utilisateur global d'un rôle de provisionnement avant de supprimer des comptes, vous pouvez répertorier les comptes de l'utilisateur global. Cliquez avec le bouton droit de la souris sur l'utilisateur global et sélectionnez Fenêtre de liste de comptes.

- La liste des comptes contient les rôles de provisionnement auxquels chaque compte appartient. Si un compte appartient à un seul rôle de provisionnement, il sera supprimé si vous supprimez l'utilisateur de ce rôle et que vous acceptez l'action de synchronisation des utilisateurs pour supprimer les comptes.
- Si un compte n'appartient à aucun rôle de provisionnement, il s'agit d'un compte supplémentaire et sera signalé par la fonctionnalité Check User Synchronization (Vérifier la synchronisation des utilisateurs). Le compte est supprimé si vous sélectionnez l'élément de menu Synchronize the User with Roles (Synchroniser l'utilisateur avec des rôles) de l'utilisateur global.

Utilisation de la suppression en attente

Vous pouvez configurer CA IdentityMinder sur un terminal après l'autre ; ainsi les comptes sur un terminal ne seront pas supprimés lorsque les administrateurs initialiseront des actions de suppression ou de synchronisation qui en règle générale supprimeraient ces comptes. En revanche, l'état de ces comptes sont définis sur Suppression en attente dans CA IdentityMinder et sur Suspension dans le terminal géré.

Les comptes définis sur Suppression en attente peuvent être identifiés dans le gestionnaire de provisionnement, dans l'onglet Statistiques des propriétés de compte. Un compte suspendu a un motif suspendu Suppression en attente et un horodatage d'entrée de cet état. Le stockage du statut Suppression en attente et de l'horodatage Suspension permet l'écriture d'un utilitaire qui identifie les comptes définis sur Suppression en attente et les supprime du serveur de provisionnement et ultérieurement du terminal géré.

Recréation de comptes supprimés

Si vous supprimez un compte d'un terminal géré à l'aide d'un outil différent de CA IdentityMinder, la fonctionnalité Check Account Synchronization (Vérifier la synchronisation des comptes) le signalera comme manquant, car il existe dans l'annuaire de provisionnement, mais non dans le terminal géré. Si cela se produit, recréez le compte dans le terminal en sollicitant la fonction Synchroniser les comptes avec le modèle de compte, ce qui recréera le compte à l'aide des modèles de compte associés au compte.

S'il s'agit de comptes recréés, CA IdentityMinder les journalisera comme comptes recréés. Vous pouvez identifier ces comptes différemment des comptes qui ont été mis à jour, car les administrateurs doivent savoir que des attributs différents des attributs de capacité (par exemple, des mots de passe) ont été définis sur des valeurs de modèle de compte d'origine.

Chapitre 9: Rôles de provisionnement

Ce chapitre traite des sujets suivants :

Rôles de provisionnement et modèles de compte

Pour simplifier la gestion des comptes, créez et gérez ces derniers à l'aide des modèles de compte, qui sont utilisés dans les rôles de provisionnement. Un rôle de provisionnement contient un ou plusieurs modèles de compte. Lorsque vous appliquez ce rôle à un utilisateur, ce dernier reçoit les comptes tels qu'ils ont été définis par les modèles.

Ces modèles servent de base aux comptes d'un type de terminal spécifique. Ils offrent le même type de fonctionnalités que les stratégies de provisionnement fournies dans eTrust Admin.

Les modèles de compte permettent d'effectuer les opérations suivantes.

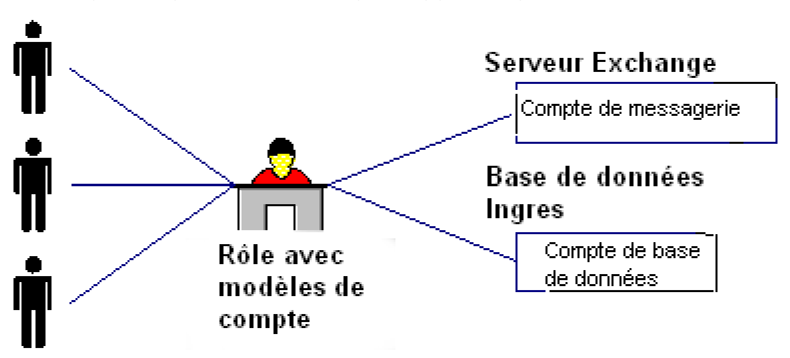
- Contrôle des attributs de compte dont disposent les utilisateurs de CA IdentityMinder sur un terminal lorsque leurs comptes sont créés
- Définition des attributs à l'aide des chaînes ou valeurs de règle
- Association des attributs de compte de différents rôles de provisionnement, afin que les utilisateurs disposent d'un seul compte, sur un terminal spécifique, avec tous les attributs de compte nécessaires
- Création ou mise à jour des attributs de compte lorsque les utilisateurs globaux modifient les rôles de provisionnement
- Synchronisation des attributs de compte afin que les utilisateurs globaux ne disposent que des attributs dont ils ont besoin
- Envoi de requêtes pour identifier les comptes à créer, à mettre à jour ou à supprimer lors d'une synchronisation
- Spécification des attributs de compte pouvant ou non être synchronisés avec les rôles de provisionnement

Création de rôles pour affecter des comptes

Dans la plupart des organisations, les administrateurs consacrent beaucoup de temps à fournir aux utilisateurs des comptes de connexion pour différents systèmes et applications. Pour simplifier cette activité répétitive, vous pouvez créer des rôles de provisionnement. Ces rôles contiennent des modèles de compte. Les modèles définissent les attributs qui existent dans un type de compte. Par exemple, un modèle de compte pour un compte Exchange définit des attributs tels que la taille de la boîte aux lettres. Les modèles de compte définissent également la manière dont les attributs d'utilisateurs sont mappés vers les comptes.

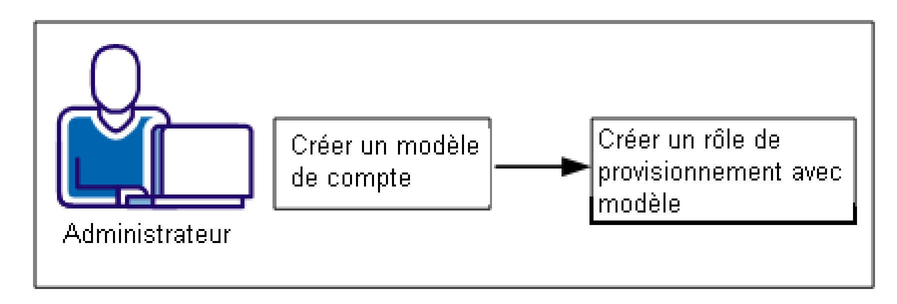
Par exemple, lorsque tous les employés de Forward, Inc ont besoin d'accéder à une base de données et à la messagerie électronique. Un administrateur veut éviter de créer un compte de base de données et un compte de messagerie pour chaque employé, un après l'autre. Il crée alors un rôle de provisionnement pour cette société. Le rôle contient un modèle de compte pour Microsoft Exchange Server, afin de fournir des comptes de messagerie et un modèle pour une base de données Oracle. Dans cet exemple, le serveur Exchange et la base de données Oracle sont des terminaux nommés qui représentent le système ou l'application sur lesquels les comptes sont créés.

Remarque : Forward, Inc est un nom de société fictif utilisé strictement à des fins d'exemple uniquement et n'est pas supposé représenter aucune société existante.



Après la création des rôles, les administrateurs de l'entreprise, tels que les gestionnaires ou le personnel du support, peuvent affecter ces rôles à des utilisateurs pour leur fournir des comptes sur des terminaux. Une fois que les utilisateurs reçoivent le rôle, ils peuvent se connecter au terminal.

La création d'un rôle de provisionnement qui inclut un modèle de compte est un processus en deux étape :



Les sections suivantes décrivent la procédure de création d'un rôle que vous pouvez utiliser pour affecter des comptes :

1. Création d'un modèle de compte (page 219)
2. Création d'un rôle de provisionnement (page 220)

Création d'un modèle de compte

Un modèle de compte par défaut pour chaque type de terminal est installé avec le serveur CA IdentityMinder. Dans un rôle de provisionnement, vous pouvez utiliser le modèle de compte par défaut ou créer vos propres modèles de compte pour tout terminal que vous avez configuré.

Pour créer un modèle de compte :

1. Sélectionnez Terminaux, Modèles de compte, Créer un modèle de compte.
2. Sélectionnez un type de terminal pour le modèle.
3. Définissez le nom du terminal comme nom système du terminal ou de l'hôte local si cela est applicable.
4. Complétez les champs dans les onglets ou utilisez les valeurs par défaut.

   Chaque type de terminal offre un ensemble d'onglets différent. Pour afficher les définitions de champs, cliquez sur Aide.
5. Sélectionnez un terminal à utiliser dans l'onglet Terminaux.
6. Cliquez sur Soumettre.

Création d'un rôle de provisionnement

Vous créez un rôle de provisionnement une fois que vous avez défini les besoins liés au rôle :

- Utilisateurs nécessitant d'autres comptes
- Comptes associés au rôle
- Membres, administrateurs et propriétaires du rôle

Création d'un rôle de provisionnement

1. Dans la console d'utilisateur, cliquez sur Rôles et tâches, Rôles de provisionnement, puis Créer un rôle de provisionnement.

   Pour obtenir des détails sur chaque onglet, cliquez sur le lien Aide de la fenêtre.

2. Remplissez l'onglet Profil. Seul le champ Nom est obligatoire.

   Remarque : Vous pouvez spécifier des attributs personnalisés dans l'onglet Profil qui indiquent des informations supplémentaires sur les rôles de provisionnement. Vous pouvez utiliser ces dernières pour faciliter les recherches de rôles dans les environnements comprenant un nombre important de rôles.

3. Remplissez l'onglet Modèles de comptes.

   a. Cliquez sur un type de terminal, tel qu'un terminal ActiveDirectory.

   b. Cliquez sur un modèle de compte.

      Les modèles que vous pouvez choisir sont basés sur le type de terminal.

   c. Ajoutez plus de modèles de comptes, selon les besoins des différents types de terminaux.

4. Renseignez l'onglet Rôles de provisionnement si vous souhaitez inclure des rôles de provisionnement dans cet onglet.

   Cette étape requiert que vous ayez activé des rôles imbriqués (page 225) pour cet environnement.

5. Remplissez l'onglet Administrateurs en ajoutant des règles d'administration qui déterminent quelles personnes gèrent les membres et les administrateurs de ce rôle.

6. Remplissez l'onglet Propriétaires en ajoutant des règles de propriété qui déterminent quelles personnes peuvent modifier ce rôle.

7. Cliquez sur Soumettre.

8. Pour vérifier que le rôle a été créé, cliquez sur Rôles de provisionnement, puis sur Afficher le rôle de provisionnement.

Tâches associées aux rôles et aux modèles

Dans la console d'utilisateur, vous pouvez créer et gérer des rôles de provisionnement en sélectionnant Rôles et tâches, puis une tâche sous Rôles de provisionnement. Des tâches existent pour les opérations standard, telles que la définition d'un utilisateur comme membre d'un rôle et la modification/suppression d'un rôle.

Avant de créer un rôle de provisionnement, vous devez disposer d'un modèle de compte à inclure dans ce rôle ou d'un rôle de provisionnement à importer. Vous pouvez importer des rôles créés dans le gestionnaire de provisionnement ou eTrust Admin. Toutefois, CA IdentityMinder ne prend pas en charge les rôles imbriqués créés dans eTrust Admin.

Importation d'un rôle de provisionnement

Bien que les rôles de provisionnement soient gérés dans la console d'utilisateur, certains rôles de provisionnement peuvent avoir été créés dans le gestionnaire de provisionnement ou une application externe. Pour ces rôles de provisionnement, vous pouvez réinitialiser le propriétaire de rôle sur un administrateur CA IdentityMinder pour pouvoir le gérer dans la console d'utilisateur.

Création d'un rôle de provisionnement

1. Connectez-vous à la console d'utilisateur en tant qu'utilisateur disposant du rôle Gestionnaire de systèmes. Cliquez sur Rôles et tâches.
2. Cliquez sur Rôles de provisionnement, Réinitialiser les propriétaires de rôle de provisionnement, puis sélectionnez un rôle de provisionnement créé dans le gestionnaire de provisionnement.
3. Remplissez l'onglet Propriétaires en ajoutant des règles de propriété qui déterminent quelles personnes peuvent modifier ce rôle.
4. Cliquez sur Soumettre.

Le rôle peut à présent être modifié, affecté ou affiché à l'aide des tâches figurant dans la catégorie Rôles de provisionnement.

Affectation de nouveaux propriétaires aux rôles de provisionnement

Vous pouvez sélectionner un ou plusieurs rôles de provisionnement et affecter des stratégies de propriété pour contrôler les utilisateurs autorisés à modifier les rôles.

Pour affecter de nouveaux propriétaires aux rôles de provisionnement :

1. Connectez-vous à la console d'utilisateur en tant qu'utilisateur disposant du rôle Gestionnaire de systèmes.
2. Cliquez sur Rôles et tâches.
3. Cliquez sur Rôles de provisionnement, puis sur Créer des stratégies de propriété pour les rôles de provisionnement.
4. Sélectionnez un ou plusieurs rôles de provisionnement.
5. Remplissez l'onglet Propriétaires en ajoutant des règles de propriété qui déterminent quelles personnes peuvent modifier ce rôle.
6. Cliquez sur Soumettre.

Les utilisateurs qui satisfont aux nouvelles stratégies de propriété peuvent modifier les rôles de provisionnement sélectionnés.

Mots de passe des comptes créés par des rôles de provisionnement

Lorsqu'un utilisateur est affecté à un rôle de provisionnement, la création d'un compte pour cet utilisateur échoue si le mot de passe de l'utilisateur CA IdentityMinder ne respecte pas les exigences relatives au mot de passe du terminal. Cela inclut la création d'un utilisateur avec un mot de passe temporaire.

Par conséquent, définissez la stratégie de mot de passe de CA IdentityMinder de sorte qu'elle corresponde à un sous-ensemble plus strict de la stratégie de mot de passe de terminal. Lors de la connexion suivante à la console d'utilisateur, vous êtes invité à remplacer le mot de passe par un mot de passe respectant les exigences de terminal.

Ordre de traitement des événements de rôle de provisionnement

Certaines tâches CA IdentityMinder par défaut incluent des *événements*, c'est-à-dire des actions que CA IdentityMinder exécute pour effectuer une tâche, qui déterminent l'appartenance à un rôle de provisionnement. Par exemple, la tâche Modifier l'utilisateur par défaut inclut AssignProvisioningRoleEvent et RevokeProvisioningRoleEvent. L'affectation ou le retrait d'un rôle de provisionnement ajoute ou supprime un compte d'un terminal. Dans certains cas, le terminal peut nécessiter que toutes les actions Ajouter soient antérieures aux actions Supprimer.

Pour forcer CA IdentityMinder à traiter les actions Ajouter en premier, activez le paramètre Cumul des événements Provisionnement de l'appartenance à un rôle dans la console de gestion. Lorsque ce paramètre est activé, CA IdentityMinder cumule les actions Ajouter et Supprimer en un seul événement, appelé AccumulatedProvisioningRolesEvent. Par exemple, si la tâche Modifier l'utilisateur affecte un utilisateur à trois rôles de provisionnement et supprime cet utilisateur de deux autres rôles, un événement AccumulatedProvisioningRolesEvent contenant cinq actions (3 actions Ajouter et 2 actions Supprimer) est généré.

Lorsque cet événement est exécuté, les actions Ajouter sont combinées en une seule opération et envoyées au serveur de provisionnement pour traitement. Une fois le traitement des actions Ajouter terminé, CA IdentityMinder combine les actions Supprimer en une seule opération qu'il envoie au serveur de provisionnement.

L'activation de ce paramètre affecte les fonctionnalités CA IdentityMinder ci-dessous.

- **Onglet Rôles de provisionnement des tâches de l'utilisateur**

  Lorsqu'un administrateur ajoute ou supprime un utilisateur d'un rôle de provisionnement à l'aide de l'onglet Rôles de provisionnement, CA IdentityMinder cumule ces actions en un seul événement.

- **Stratégies d'identité**

  Tous les événements d'appartenance aux rôles de provisionnement (AssignProvisioningRoleEvent ou RevokeProvisioningRoleEvent) générés suite à l'évaluation d'une stratégie d'identité sont cumulés en un événement AccumulatedProvisioningRolesEvent. CA IdentityMinder exécute cet événement comme tout autre événement secondaire. Prenons l'exemple d'un ensemble de stratégies d'identité incluant deux stratégies d'identité : la stratégie A retire l'appartenance au rôle de provisionnement A et la stratégie B affecte les utilisateurs au rôle de provisionnement B. Si CA IdentityMinder détermine qu'un utilisateur n'est plus conforme à la stratégie A mais à la stratégie B, un événement AccumulatedProvisioningRolesEvent contenant deux actions (une pour l'action Supprimer, une autre pour l'action Ajouter) est généré. L'action Ajouter est exécutée avant l'action Supprimer.

- **Affichage des tâches soumises**

  Pour afficher l'état de l'événement AccumulatedProvisioningRolesEvent et celui de chaque action, utilisez la tâche Afficher les tâches soumises pour afficher les détails de l'événement.

  Si l'une des actions échoue, l'état Echec est affecté à l'événement, ainsi qu'à la tâche.

- **Flux de travaux**

  Vous pouvez associer un processus de flux de travaux à l'événement AccumulatedProvisioningRolesEvent. Dans ce cas, un approbateur peut approuver ou rejeter l'événement et par conséquent les événements sous-jacents.

  Une configuration supplémentaire est nécessaire pour activer le flux de travaux des événements appartenant à l'événement AccumulatedProvisioningRolesEvent.

- **Audit**

  CA IdentityMinder audite les informations relatives à l'événement AccumulatedProvisioningRolesEvent et aux événements sous-jacents.

Activation de l'accumulation des événements d'appartenance à un rôle de provisionnement

CA IdentityMinder fournit un paramètre de configuration dans la console de gestion qui active la combinaison de toutes les actions Ajouter et Supprimer d'un événement d'appartenance à un rôle de provisionnement en une seule opération. Une fois les actions combinées, CA IdentityMinder traite les actions Ajouter comme une seule opération avant de traiter les actions Supprimer.

Ce paramètre permet le séquencement des événements requis par certains types de terminaux.

Remarque : Par défaut, cette option est désactivée.

Pour activer l'accumulation des événements d'appartenance à un rôle de provisionnement :

1. Accédez à la console de gestion Identity Manager.
2. Cliquez sur Environnements.
3. Sélectionnez l'environnement à configurer.
4. Ouvrez Paramètres avancés, Provisionnement.
5. Activez la case à cocher Activer l'accumulation des événements d'appartenance à un rôle de provisionnement.
6. Redémarrez le serveur d'applications.

Activation des rôles imbriqués dans un environnement

Vous pouvez inclure un rôle de provisionnement dans un autre rôle de provisionnement. Le rôle inclus est appelé rôle imbriqué.

Par exemple, vous pouvez créer un rôle de provisionnement Employé. Ce rôle Employé fournit les comptes nécessaires à tous les employés, tels que les comptes de messagerie. Vous incluez le rôle Employé dans des rôles de provisionnement spécifiques de service, tels que des rôles Finance et Ventes. Les rôles de provisionnement de service fournissent des comptes uniquement associés à ce service. Cette combinaison de rôles fournit les comptes appropriés à chaque utilisateur.

Pour activer des rôles imbriqués dans un environnement

1. Dans la console de gestion, sélectionnez l'environnement.
2. Cliquez sur Paramètres de tâches et de rôles, Importer.
3. Sélectionnez Prise en charge des rôles de provisionnement imbriqués.
4. Cliquez sur Terminer.
5. Redémarrez l'environnement.

Inclusion d'un rôle dans un rôle de provisionnement

Pour inclure un rôle dans un rôle de provisionnement

1. Cliquez sur Rôles et tâches, Rôles de provisionnement, Modifier le rôle de provisionnement.
2. Renseignez l'onglet Rôles de provisionnement en cliquant sur Ajouter un rôle, puis sélectionnez un rôle de provisionnement.

   Pour des raisons de performances, nous vous recommandons de limiter l'imbrication de rôles à trois niveaux. Par exemple, vous appartenez au rôle de provisionnement actuel (le rôle de premier niveau) et à un autre rôle (le rôle de deuxième niveau), qui peut quant à lui inclure un rôle de troisième niveau. Nous vous recommandons de n'inclure aucun rôle dans le rôle de troisième niveau.
3. Renseignez la stratégie de propriétaire en modifiant la règle de propriété.

   La portée doit être égale ou supérieure à celle du rôle ajouté.
4. Cliquez sur Soumettre.

Attributs des modèles de compte

Les attributs des modèles de compte déterminent la définition des attributs dans le compte.

Attributs de capacité et initiaux

Les modèles de compte incluent deux types d'attributs.

- *Les attributs de capacités* représentent les informations de compte, telles que la taille de stockage, la quantité, les limites de fréquence ou les appartenances aux groupes. Le gestionnaire de provisionnement met en évidence les attributs de capacité sur toutes les fenêtres de modèle de compte pour faciliter leur identification.
- Les *attributs initiaux* représentent toutes les informations initialement définies pour un compte (nom, mot de passe et état du compte), ainsi que des informations personnelles (nom, adresse et numéros de téléphone).

Les comptes sont synchronisés avec leur modèles de compte en même temps que tous les attributs de capacité. Il s'agit d'attributs différents d'un type de terminal à un autre, comme les appartenances aux groupes, les droits, les quotas, les restrictions de connexion, qui contrôlent les activités qu'un utilisateur peut effectuer lorsqu'il se connecte au compte.

La synchronisation ne met pas à jour les autres attributs de compte. Ceux-ci sont initialisés à partir des modèles de compte lors de la création des comptes et mis à jour via les fonctions de propagation. Le serveur de provisionnement inclut deux fonctions de propagation : une première mise à jour immédiate des comptes lors de la modification du modèle de compte et une seconde mise à jour lors de la modification des attributs d'utilisateur globaux.

Recherche d'attributs de capacité et initiaux

Pour rechercher les attributs définis comme fonctionnalités et initiaux, vous devez générer le fichier eTACapability.txt. Entrez la commande suivante dans l'invite de commande Windows :

```
PS_HOME\dumpptt.exe -c > eTACapability.txt
```

PS_Home

Spécifie C:\Program Files\CA\Identity Manager\Provisioning Server\bin.

Une version du fichier est générée pour tous les connecteurs que vous avez installés.

Chaînes de règle pour les attributs

Les attributs de compte sont générés à l'aide de chaînes de règle, dont les variables sont remplacées par la valeur correspondant au compte concerné. Les chaînes de règle sont utiles lorsque vous voulez générer des attributs de compte différents. Lorsque les règles sont évaluées, CA IdentityMinder remplace les chaînes de règle des modèles de compte par les données spécifiées dans l'objet de l'utilisateur global.

Remarque : L'évaluation des règles n'est pas effectuée sur les comptes créés lors d'une exploration ou sans rôle de provisionnement.

Les noms de compte devant être uniques, entrez une chaîne de règle %AC% dans le champ Nom du compte d'un modèle de compte. Lorsque CA IdentityMinder crée un compte à l'aide de ce modèle de compte, il utilise le nom de compte de l'utilisateur.

Le tableau suivant répertorie les chaînes de règle dans CA IdentityMinder.

Chaîne de règle	Description
%AC%	Nom du compte
%D%	Date actuelle au format *jj/mm/aaaa.* La date est une valeur calculée qui ne tient pas compte des informations de l'utilisateur global. Cette chaîne de règle ressemble à ce qui suit. %$$DATE()% %$$DATE%
%EXCHAB%	Boîte aux lettres masquée dans le carnet d'adresses Exchange
%EXCHS%	Nom du serveur de boîtes aux lettres
%EXCMS%	Nom de la banque de boîtes aux lettres
%GENUID%	ID d'utilisateur UNIX/POSIX numérique. Cette variable de règle est identique à %UID% tant que la valeur ID unique de l'utilisateur global est définie. Toutefois, si l'utilisateur global n'est associé à aucune valeur d'ID unique et que la génération de celui-ci est activée (dans les propriétés globales de la tâche Système), le prochain ID unique disponible est affecté à l'utilisateur global et sert de valeur pour cette variable de règle.
%P%	Mot de passe
%U%	Nom d'utilisateur global
%UA%	Adresse complète (générée à partir de la rue, de la ville, du pays et du code postal)
%UB%	Bâtiment
%UC%	Ville
%UCOMP%	Nom de la société

Chaîne de règle	Description
%UCOUNTRY%	Pays
%UCU*xx*% or %UCU*xxx*%	Champ personnalisé (*xx* ou *xxx* représente l'ID de champ à 2 ou 3 chiffres comme spécifié dans l'onglet Champs d'utilisateur personnalisé de la tâche Système)
%UD%	Description
%UDEPT%	Service
%UE%	Adresse électronique
%UEP%	Adresse électronique principale
%UES%	Adresses électroniques secondaires
%UF%	Prénom
%UFAX%	Numéro de télécopie
%UHP%	Page d'accueil
%UI%	Initiales
%UID%	ID d'utilisateur UNIX/POSIX numérique.
%UL%	Nom
%ULOC%	Emplacement
%UMI%	Initiales des prénoms secondaires
%UMN%	Deuxième prénom
%UMP%	Portable
%UN%	Nom complet
%UO%	Nom du bureau
%UP%	Numéro de téléphone
%UPAGE%	Récepteur d'appels
%UPC%	Code postal
%UPE%	Numéro de poste
%US%	Etat
%USA%	Adresse (rue)
%UT%	le poste ;

Chaîne de règle	Description
%XD%	Génère l'horodatage actuel au format XML dateTimeValue (chaîne à longueur fixe). Dans un attribut dateValue ou timeValue, vous pouvez écrire une expression de sous-chaîne (:offset,length) pour extraire la date ou l'heure de dateTimeValue. Par exemple, %XD:1,10% renvoie AAAA-MM-JJ et %XD:12,8% renvoie HH:MM:SS.

Valeurs pour les attributs

Pour utiliser une valeur constante pour un attribut de compte, entrez la valeur dans le champ de modèle de compte plutôt que dans une chaîne de règle. Par exemple, vous pouvez entrer des valeurs pour spécifier les limites de fréquence ou une quantité.

Si la valeur d'attribut constante doit contenir plusieurs signes de pourcentage, entrez deux signes de pourcentage (%%) à chaque fois. CA IdentityMinder les traduit en un signe de pourcentage (%) lorsque vous créez la valeur d'attribut de compte. Si la valeur de modèle de compte contient un seul signe de pourcentage, CA IdentityMinder ne génère pas d'erreur. La règle indique que vous devez spécifier 25 %% si vous voulez une valeur littérale de 25 %. Il se peut que 25 % soit accepté dans certains cas.

Expressions de règle avancées

Pour une flexibilité accrue par rapport à la simple substitution des attributs d'utilisateur global, vous pouvez entrer des expressions de règle avancées, notamment ce qui suit.

- Sous-chaînes des expressions de règle utilisant le décalage et la longueur
- Combinaisons de chaînes et de valeurs de règle
- Expressions de règle permettant de définir plusieurs valeurs pour des attributs de compte à plusieurs valeurs
- Variables de règle pour les autres attributs de l'utilisateur global
- Invocation des fonctions intégrées
- Invocation des fonctions de sortie de programme écrites par le client

Association de chaînes de règle et de valeurs

Vous pouvez associer des chaînes de règle et des valeurs de constantes en une valeur d'attribut de modèle de compte. Par exemple, s'il n'y a aucune chaîne de règle %UI%, vous pouvez obtenir le même résultat en concaténant plusieurs expressions de règle comme suit.

```
%UF:,1%%UMI:,1%%UL:,1%
```

La chaîne de règle %UA% ressemble à ce qui suit.

```
%USA%, %UC%, %US%, %UPC%
```

Vous pouvez également associer une chaîne de règle à une valeur de constante pour créer un attribut de terminal de base UNIX comme suit.

```
/u/home/%AC%
```

Sous-chaînes de règle

La syntaxe suivante permet de créer une valeur de sous-chaîne ou une variable de règle.

`%`*`var`*`[:`*`décalage`*`,`*`longueur`*`]%`

var

Représente le nom de la variable de règle prédéfinie telle que définie dans la table montrée précédemment.

décalage

(Facultatif) Définit le décalage de départ du suffixe de sous-chaîne. Le chiffre 1 représente le premier caractère.

longueur

(Facultatif) Définit le décalage de fin du suffixe de sous-chaîne. L'utilisation d'un astérisque (*) comme valeur de longueur indique la fin de la valeur.

Par exemple, pour définir un attribut de compte sur les quatre premiers caractères de l'attribut Bâtiment d'un utilisateur global, utilisez la syntaxe suivante pour définir la variable.

```
%UB:1,4%
```

Si l'attribut Bâtiment est vide ou comporte moins de quatre caractères, la valeur d'attribut de compte qui en résulte aura moins de quatre caractères.

Expressions de règle à valeurs multiples

La plupart des expressions de règle comportent une seule valeur. Elles sont issues d'une valeur d'attribut d'utilisateur (éventuellement vide) et ont pour résultat une valeur d'attribut de compte (éventuellement vide également). Toutefois, il est possible de considérer un attribut d'utilisateur vide comme une valeur nulle. Il est également possible de générer plusieurs valeurs pour renseigner une valeur d'attribut de compte à valeurs multiples.

La syntaxe de règle suivante permet d'utiliser ou non les valeurs qu'un attribut d'utilisateur peut contenir.

%**var*%

L'astérisque facultatif signalant la prise en charge des valeurs multiples (*), situé immédiatement après le premier signe % de l'expression de règle, indique que le résultat doit être 0, 1 ou plusieurs valeurs en fonction du nombre de valeurs que l'attribut d'utilisateur référencé contient.

La plupart des attributs d'utilisateur comportent une seule valeur. Ils peuvent soit contenir une seule valeur, soit n'en contenir aucune. Les attributs personnalisés (Champ_personnalisé_01 à Champ_personnalisé_99) comportent plusieurs valeurs. Une variable de règle qui fait référence à ces attributs peut soit contenir une ou plusieurs valeurs, soit n'en contenir aucune.

Si un attribut d'utilisateur comporte plusieurs valeurs mais que vous omettez l'astérisque (*) dans l'expression de règle, le résultat de l'évaluation des règles correspond à celui de la première valeur. Toutefois, dans la plupart des cas, les valeurs d'attribut sont officiellement non triées, de sorte que la première valeur considérée par CA IdentityMinder peut être imprévisible.

Si un attribut d'utilisateur comporte plusieurs valeurs et que vous incluez l'astérisque dans l'expression de règle, plusieurs valeurs sont générées pour l'attribut de compte. Ne définissez pas une expression de règle à plusieurs valeurs dans un modèle de compte si l'attribut de compte défini à partir de l'attribut du modèle ne comporte pas lui-même plusieurs valeurs.

Vous pouvez définir un attribut de compte étendu dans le type de terminal ADS de sorte qu'il comporte plusieurs valeurs, puis utiliser cette syntaxe d'expression de règle à plusieurs valeurs pour définir cet attribut. Prenez l'exemple d'un environnement qui définit un attribut de compte ADS étendu nommé "brevets" et un troisième attribut d'utilisateur personnalisé également nommé "brevets".

Un modèle de compte ADS peut définir, pour l'attribut "brevets", la chaîne de règle %*UCU03%. Vous pouvez ensuite modifier l'attribut "brevets" d'un utilisateur en ajoutant une ou plusieurs valeurs. Lorsque vous appliquez les modifications à l'utilisateur, sélectionnez la mise à jour des comptes de l'utilisateur. Cette option consulte le modèle du compte, identifie la variable de règle %*UCU03%, et copie tous les brevets de l'utilisateur dans l'attribut "brevets" du compte.

De la même manière, les chaînes de règle sont évaluées lors de la création d'un compte. Par ailleurs, lors de la modification du modèle de compte, vous pouvez choisir de recalculer la règle pour tous les comptes associés au modèle de compte si la chaîne de règle est modifiée.

La syntaxe %**var*% est également utile pour les variables *var* qui font référence aux attributs d'utilisateur comportant une seule valeur. Cela s'applique uniquement en cas de concaténation et si les attributs référencés ne sont pas définis pour les utilisateurs.

L'astérisque facultatif signalant la prise en charge des valeurs multiples (*) indique que la règle contenant une variable de règle %**var*% ne donne aucune valeur si l'attribut d'utilisateur ne comporte aucune valeur. En revanche, l'expression de règle comportant une seule valeur %*var*% donne toujours une seule valeur, même s'il s'agit d'une chaîne vide.

Pour comprendre cette différence, considérez les chaînes de règle suivantes.

```
(310)%UP%
 (310)%*UP%
```

A priori, les deux chaînes de règle ajoutent l'indicatif 310 au numéro de téléphone. Elles sont pourtant différentes, car si les utilisateurs n'ont aucune valeur pour leur numéro de téléphone, la première règle donne la valeur de compte (310). La deuxième chaîne de règle ne génère aucune valeur et laisse l'attribut de compte indéfini.

A présent, considérez les chaînes de règle suivantes qui ajoutent le numéro de poste au numéro de téléphone :

```
%UP% %UPE%
%UP% %*UPE%
```

Si tous les utilisateurs ont un numéro de téléphone mais que certains d'entre eux n'ont pas de poste, la première règle de chaîne génère une valeur qui inclut le numéro de téléphone de chaque utilisateur, sans poste. La deuxième chaîne de règle ne génère aucune valeur. Dans ce cas, utilisez la première règle avec %UPE%.

Règles d'attribut d'utilisateur global explicites

Chaque utilisateur dispose d'autres attributs en plus de ceux répertoriés dans la table des règles précédente. Il est peu probable que vous deviez créer des expressions de règle faisant référence à l'un de ces autres attributs. Vous pouvez toutefois utiliser la syntaxe suivante pour faire référence à un attribut d'utilisateur spécifique.

```
%#ldap-attribute%
```

Par exemple, si vous devez définir la valeur du champ Suspendu d'un utilisateur, vous pouvez déterminer le nom d'attribut LDAP correspondant (à savoir, eTSuspended) et créer l'expression de règle qui donne 0 ou 1, comme eTSuspended.

```
%#eTSuspended%
```

Vous pouvez également identifier les rôles de provisionnement affectés à l'utilisateur à l'aide de l'expression de règle ci-dessous.

```
%*#eTRoleDN%
```

Ces rôles de provisionnement correspondent à des valeurs de nom unique LDAP complet. Il se peut que les valeurs soient plus utiles lorsqu'elles sont associées à la fonction intégrée RDNVALUE (reportez-vous au tableau suivant). L'astérisque (*) signalant la prise en charge des valeurs multiples permet d'identifier tous les rôles de provisionnement affectés à l'utilisateur sous la forme de valeurs multiples.

La syntaxe de sous-chaîne est également applicable à ces expressions de règle. Par exemple, vous pouvez utiliser %#eTTelephone:6,*% à la place de %UP:6,*. L'une et l'autre demandent à CA IdentityMinder d'extraire les cinq premiers caractères du champ Téléphone de l'utilisateur.

Fonctions de règle intégrées

Vous pouvez utiliser les fonctions de règle intégrées dans vos expressions de règle pour effectuer diverses transformations sur les valeurs. La forme générale d'invocation d'une fonction de règle intégrée est

```
%[*]$$fonction(arg[,…])[:décalage,longueur]%
```

où l'astérisque signalant la prise en charge des valeurs multiples (*) et les spécifications des sous-chaînes de décalage et de longueur sont facultatifs.

Les fonctions intégrées reconnues sont les suivantes.

Fonction de règle intégrée	Description
ALLOF	Fusionne tous les paramètres en un attribut à plusieurs valeurs. L'ordre est conservé et les doublons sont supprimés. Par exemple, si les attributs d'utilisateur sont définis comme suit : eTChamp_personnalisé_01: { A, B } eTChamp_personnalisé_02: { A, C } la règle : %*ALLOF(%*UCU01%,%*UCU02%)% donne les trois valeurs { A, B, C }.
DATE	Donne la valeur de la date actuelle au format *jj/mm/aaaa*. L'expression de règle %D% ressemble à ce qui suit. %$$DATE()% %$$DATE%
FIRSTOF	Renvoie la première valeur d'un paramètre quelconque. Cette fonction permet d'insérer une valeur par défaut dans le cas où un attribut n'est pas défini. %$$FIRSTOF(%UCU01%,'inconnu')% %$$FIRSTOF(%LN%,%UCU01%,%U%)% Si aucune de ces valeurs n'est définie, aucune valeur n'est prise en compte. Pour entrer une chaîne constante dans un argument, insérez une apostrophe de part et d'autre.
INDEX	Renvoie une valeur d'un attribut à plusieurs valeurs. Index 1 est la première valeur. Si l'index est supérieur au nombre de valeurs, le résultat est la valeur (vide) non définie. Les règles ressemblent à ce qui suit. %$$INDEX(%*UCU01%,1)% %$$FIRSTOF(%*UCU01%)%

Fonction de règle intégrée	Description
NOTEMPTY	Renvoie la valeur unique de son argument, mais signale un échec si la valeur d'attribut n'est pas définie. Exemple 1 : Faire échouer la création ou la mise à jour du compte si l'utilisateur n'a pas d'attribut UID affecté. %$$NOTEMPTY(%UID%)% Exemple 2 : Utiliser le prénom. S'il n'est pas défini, utiliser le nom de famille. Si aucun des deux n'est défini, faire échouer la création ou la mise à jour du compte. %$$NOTEMPTY(%$$FIRSTOF(%UF%, %UL%)%)%
PRIMARYEMAIL	Renvoie l'adresse électronique principale extraite de plusieurs adresses électroniques. L'expression %UE% ressemble à ce qui suit. %$$PRIMARYEMAIL(%UEP%)%
RDNVALUE	Traite la valeur d'attribut comme un nom unique LDAP et extrait le nom commun de l'objet à partir du nom unique. %*$$RDNVALUE(%#eTRoleDN%)% Renvoie les noms communs de tous les rôles de provisionnement affectés. Si l'utilisateur appartient à deux rôles de provisionnement avec le même nom commun, le nom de ce rôle est cité une fois.
TOLOWER	Convertit un texte en majuscules en texte en minuscules. %$$TOLOWER(%AC%)%
TOUPPER	Convertit un texte en minuscules en texte en majuscules. %$$TOUPPER(%U%)%

Fonction de règle intégrée	Description
TRIM	Supprime les caractères vides à gauche et à droite d'une valeur d'attribut. Par exemple, "%UF %UL%" crée généralement une valeur avec un prénom et un nom séparés par un caractère vide. Si l'utilisateur a un attribut de prénom vide, cette règle génère une valeur terminée par un caractère vide. L'utilisation de "%$$TRIM(%UF% %UL%)% garantit qu'aucun caractère vide n'apparaît à gauche ou à droite de la valeur d'attribut de compte, même si le prénom ou le nom de famille n'est pas défini.

Performances des rôles de provisionnement

Lorsque vous utilisez Identity Manager avec un serveur de provisionnement, vous pouvez tirer parti de certaines améliorations des performances de provisionnement.

Objet de cache JIAM

Identity Manager communique avec le serveur de provisionnement à l'aide de l'API Java IAM (JIAM). Pour améliorer la communication, configurez un cache pour les objets extraits du serveur de provisionnement.

Activation du cache JIAM

Pour activer le cache JIAM :

1. Accédez aux paramètres de l'environnement via la console de gestion. Cliquez sur Paramètres avancés, Divers.
2. Configurez la propriété définie par l'utilisateur pour le cache JIAM.
   - **Propriété** : JIAMCache
   - **Valeur** : true
3. Cliquez sur Ajouter.
4. Cliquez sur Enregistrer.

   La propriété définie par l'utilisateur est enregistrée.

Définition de la durée de vie du cache JIAM

Le cache JIAM stocke des informations pendant un délai spécifique avant l'expiration des données. Ce délai est appelé durée de vie. Vous pouvez définir la durée de vie du cache JIAM (en secondes) pour définir la durée de conservation des données dans le cache.

Pour tirer parti des données mises en cache localement, vous devez trouver un équilibre entre les gains de performances et les données à disposition. Une durée de vie comprise entre un et sept jours est recommandée. Pour connaître les valeurs de durée de vie à utiliser, reportez-vous au tableau ci-dessous.

Durée de vie souhaitée	Paramètres de durée de vie (en secondes)
24 heures (1 jour)	86 400
72 heures (3 jours)	259 200
120 heures (5 jours)	432 000
168 heures (7 jours)	604 800

Pour définir la durée de vie du cache JIAM :

1. Accédez à l'environnement via la console de gestion. Cliquez sur Paramètres avancés, Divers.
2. Configurez la propriété définie par l'utilisateur pour la durée de vie du cache JIAM.
   - **Propriété** : JIAMCacheTTL
   - **Valeur** : nombre de secondes de conservation des données dans le cache JIAM

     Par défaut : 300
3. Cliquez sur Ajouter.
4. Cliquez sur Enregistrer.

   La propriété définie par l'utilisateur est enregistrée.

Mise en pool des sessions

Pour améliorer les performances, Identity Manager peut affecter un nombre de sessions mises en pool lorsqu'il communique avec le serveur de provisionnement.

Pour plus d'informations sur la mise en pool des sessions, reportez-vous à l'*aide en ligne de la console de gestion*.

Tâches de provisionnement pour les environnements existants

Si vous importez des définitions de rôles personnalisées et souhaitez activer le provisionnement dans un environnement, vous devez *également* importer les définitions du rôle Provisionnement uniquement dans la console de gestion. Ces définitions de rôle sont situées dans le répertoire suivant :

`iam_im.ear\management_console.war\WEB-INF\Template\environment`

Remarque : Pour plus d'informations sur l'importation des définitions de rôle, reportez-vous au *manuel de configuration* (en anglais).

Chapitre 10: Services gérés

Ce chapitre traite des sujets suivants :

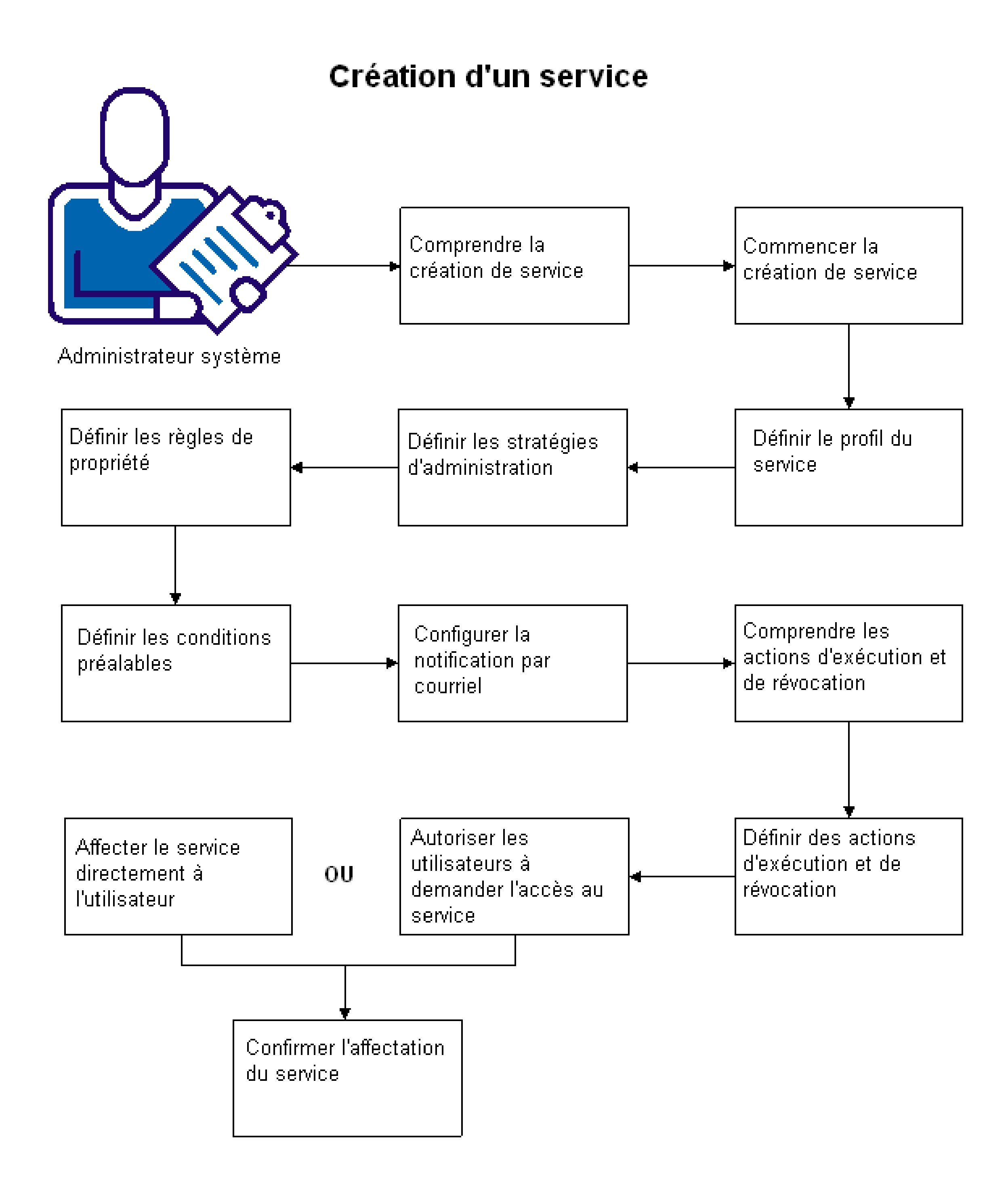
Création de service

Les services simplifient la gestion des droits. Un service regroupe tous les droits (tâches, rôles, groupes et attributs) dont un utilisateur a besoin pour un rôle professionnel donné. L'utilisateur peut accéder aux services par l'intermédiaire des tâches Demande d'accès, dans la console d'utilisateur de CA Cloud Access Manager. Les tâches Demande d'accès permettent à un utilisateur ou à un administrateur de demander, d'affecter, de retirer et de renouveler un service.

Les services permettent aux administrateurs de combiner des droits d'utilisateur dans un package unique et de les gérer comme un ensemble. Par exemple, tous les nouveaux employés des ventes ont besoin d'accéder à un ensemble défini de tâches et de comptes sur des systèmes d'extrémité spécifiques. Ils ont également besoin d'informations spécifiques qui doivent être ajoutées à leurs profils de compte d'utilisateur. Un administrateur crée un service nommé Administration des ventes, contenant toutes les tâches, les rôles, les groupes et les informations d'attribut de profil requis pour un nouvel employé des ventes. Lorsqu'un administrateur affecte le service Administration des ventes à un utilisateur, cet utilisateur reçoit l'intégralité de l'ensemble des rôles, tâches, groupes et attributs de compte définis par le service.

Les utilisateurs peuvent également accéder aux services en effectuant eux-mêmes une demande d'accès. Dans la console d'utilisateur, chaque utilisateur dispose d'une liste des services disponibles qu'il peut demander. Cette liste contient les services définis sur Auto-abonnement par un administrateur avec des droits appropriés, généralement pendant la création du service. A partir de la liste des services disponibles, les utilisateurs peuvent demander l'accès aux services dont ils ont besoin. Lorsqu'un utilisateur demande l'accès à un service, la demande est exécutée automatiquement et les droits associés sont affectés à l'utilisateur immédiatement. Un administrateur disposant des droits appropriés peut également configurer l'exécution des services de sorte à requérir l'approbation de flux de travaux ou à générer des notifications par courriel.

Le schéma suivant contient des informations importantes et les étapes à suivre pour créer un service.


Création d'un service
Administrateur système
Comprendre la création de service
Commencer la création de service
Définir le profil du service
Définir les stratégies d'administration
Définir les règles de propriété
Définir les conditions préalables
Configurer la notification par courriel
Comprendre les actions d'exécution et de révocation
Définir des actions d'exécution et de révocation
Autoriser les utilisateurs à demander l'accès au service
OU
Affecter le service directement à l'utilisateur
Confirmer l'affectation du service

Les rubriques suivantes décrivent la procédure de création et de mise à disposition d'un service :

1. Description de la création de service (page 242)
2. Démarrage de la création de service (page 243)
3. Définition du profil de service
4. Définition de stratégies d'administration du service (page 246)
5. Définition des règles de propriété pour le service (page 247)
6. Définition des conditions préalables pour le service (page 247)
7. Configuration de la notification par courriel du renouvellement de service (page 248)
8. Description des actions d'exécution et de révocation (page 249)
9. Définition des actions d'exécution et de révocation pour le service
10. Octroi de l'accès aux services pour les utilisateurs

    Dans la console d'utilisateur, lorsque l'utilisateur clique sur Mon accès, puis sur Demander et afficher un accès, la liste des services disponibles qu'il peut demander s'affiche. Les services qui s'affichent dans cette liste sont définis sur Auto-abonnement par un administrateur avec les droits appropriés, généralement lors de la création des services.
11. Affectation d'un service directement à un utilisateur (page 89)
12. Confirmation de l'affectation du service (page 251)

Description de la création de service

Avant de créer un service, tenez compte des informations et des droits nécessaires pour créer et exécuter le service.

Posez-vous les questions suivantes :

1. Quel est l'objectif de ce service ? Par exemple, vous pouvez créer un service permettant de créer un compte Salesforce.com pour tous les nouveaux employés.
2. Les membres du service requièrent-ils certains rôles d'administration ? Si tel est le cas, créez ou identifiez ces rôles d'administration.
3. Les membres du service doivent-ils recevoir l'accès à un ou plusieurs terminaux ? Si oui, créez ou identifiez ces terminaux.
4. Si les membres du service doivent accéder à des terminaux, créez ou identifiez les rôles de provisionnement associés et les modèles de compte.

5. Les membres du service doivent-ils être membres de certains groupes ? Si oui, créez ou identifiez ces groupes.
6. Certains attributs d'utilisateur doivent-ils être référencés ou modifiés lorsqu'un utilisateur devient membre du service ? Par exemple, lorsqu'un utilisateur reçoit le service Salesforce.com, faut-il confirmer si l'attribut de département pour cet utilisateur est défini sur Ventes ? Si tel est le cas, créez ou identifiez ces attributs d'utilisateur.

Après avoir créé ou identifié ces conditions préalables, vous pouvez commencer la création de service (page 243).

Démarrage de la création de service

Vous créez un service à partir de la console d'utilisateur.

Procédez comme suit:

1. Connectez-vous à un compte disposant de droits de gestion des services.

   Par exemple, le premier utilisateur d'un environnement dispose du rôle Gestionnaire de systèmes, qui comporte la tâche Créer un service.
2. Dans le menu de navigation, sélectionnez Services.
3. Cliquez sur Gérer les services, puis sur Créer un service.
4. Définition du profil de service

Définition du profil de service

L'onglet Profil permet de définir les caractéristiques de base du service.

Procédez comme suit:

1. Entrez un nom et une balise. Une balise est un identificateur unique pour le service.

   Remarque : Les balises peuvent uniquement contenir des caractères alphanumériques et des traits de soulignement, et elles ne peuvent pas commencer par un nombre. Une fois créée, une balise de nom ne peut pas être modifiée ou réutilisée, même si un service est supprimé par la suite.
2. Sélectionnez Activé si le service peut être mis à la disposition des utilisateurs dès sa création.
3. Sélectionnez Auto-abonnement si vous voulez que ce service s'affiche dans la liste de services que les utilisateurs peuvent demander. Lorsque l'option Auto-abonnement est activée, les utilisateurs peuvent demander l'accès à ce service par l'intermédiaire de la console d'utilisateur.

4. (Facultatif) Ajoutez une ou plusieurs catégories. Saisissez un nom de catégorie et cliquez sur la flèche vers le haut pour l'ajouter au service.

   Les catégories ajoutent des informations supplémentaires à un service. Vous pouvez utiliser ces informations pour faciliter les recherches de services dans les environnements comprenant un nombre important de services.

5. Spécifiez une Fenêtre des données de l'utilisateur pour l'exécution du service pour collecter les données de l'utilisateur supplémentaires au moment où l'utilisateur demande le service.

   Utilisez une Fenêtre des données de l'utilisateur pour l'exécution du service pour vous assurer que toutes les données de l'utilisateur nécessaires pour exécuter le service existent dans le système. Par exemple, une adresse électronique valide est requise pour exécuter un service qui crée un compte dans Google Apps. Si aucune adresse électronique pour un utilisateur n'existe dans le référentiel d'utilisateurs de CA Cloud Access Manager, l'utilisateur devra la fournir lors de la demande du service.

a. Cliquez sur Parcourir.

   La liste des fenêtres de profils disponibles s'affiche. Ces fenêtres sont généralement utilisées pour collecter des données d'utilisateur.

b. Sélectionnez une fenêtre de profil qui contient les données de l'utilisateur à collecter. Choisissez une des options suivantes :

   - Cliquez sur Sélectionner pour collecter toutes les données de l'utilisateur contenues dans cette fenêtre.

   OU

   - Cliquez sur Copier pour personnaliser les données de l'utilisateur que vous voulez collecter. Spécifiez un nom et une balise unique pour la nouvelle fenêtre. Ajoutez, modifiez ou supprimez des éléments de données de l'utilisateur et cliquez sur OK.

   OU

   - Cliquez sur Modifier pour changer les données de l'utilisateur contenues dans cette fenêtre. Ajoutez, modifiez ou supprimez des éléments de données de l'utilisateur et cliquez sur OK.

   Important : Si vous modifiez une fenêtre de données de l'utilisateur, vos modifications s'appliqueront à chaque utilisation de la fenêtre dans la console d'utilisateur. Vous pouvez également copier et personnaliser la fenêtre de profil.

c. Cliquez sur Sélectionner.

   Les éléments de données de l'utilisateur que vous avez sélectionnés sont collectés au moment de la demande du service.

   Remarque : Si les données requises existent dans le système lorsque l'utilisateur effectue une demande de service, les données apparaissent dans la fenêtre de profil.

6. Définition de stratégies d'administration du service (page 246)

Définition de stratégies d'administration du service

Dans l'onglet Administrateurs, vous pouvez définir les utilisateur autorisés à ajouter ou à supprimer des utilisateurs tels que les membres et les administrateurs de ce service. Les stratégies d'administration contiennent les règles de portée et d'administration et au moins un droit d'administrateur (Gérer les membres ou Gérer les administrateurs).

Les règles d'administration définissent les personnes qui peuvent administrer ce service. Les règles de portée définissent les utilisateurs qui peuvent devenir administrateurs. Par exemple, une règle d'administrateur peut autoriser tous les membres du groupe Ventes à administrer un service. Une règle de portée peut alors limiter ces utilisateurs à uniquement des membres du groupe Ventes à Boston, aux Etats-Unis, par exemple.

Procédez comme suit:

1. Dans l'onglet Administrateurs, cliquez sur Ajouter.

   La fenêtre Stratégie d'administration s'ouvre.

2. Définissez une règle d'administration selon laquelle les utilisateurs peuvent administrer ce service. Par exemple, vous pouvez spécifier des utilisateurs membres du groupe Ventes ou des utilisateurs disposant de l'attribut de profil spécifique du poste Directeur commercial.

   Cliquez sur la flèche vers la gauche pour modifier une portion de règle préalablement spécifiée.

3. Définissez une règle de portée pour définir les utilisateurs qui peuvent administrer ce service. Par exemple, si vous avez spécifié des utilisateurs membres du groupe Ventes dans la règle d'administration, vous pouvez alors limiter l'étendue de cette règle uniquement aux utilisateurs dont la ville est Boston, Etats-Unis.

   Remarque : Vous pouvez ajouter plusieurs stratégies d'administration avec des règles et des droits différents pour chaque service.

4. Si vous voulez autoriser les administrateurs à ajouter ou à supprimer des membres de ce service, cliquez sur Possibilité de gérer les membres de ce service.

5. Cliquez sur OK.

6. Pour modifier davantage une stratégie, cliquez sur l'icône Modifier. Pour supprimer une stratégie, cliquez sur l'icône du signe moins.

7. Définition des règles de propriété pour le service (page 247)

Définition des règles de propriété pour le service

Dans l'onglet Propriétaires, vous définissez des règles sur les personnes qui peuvent devenir propriétaires du service. Un propriétaire est un utilisateur qui peut modifier le service.

Procédez comme suit:

1. Dans l'onglet Propriétaires, cliquez sur Ajouter.

   La fenêtre Règle de propriété s'affiche.

2. Définissez une règle de propriété selon laquelle les utilisateurs peuvent posséder ce service. Par exemple, vous pouvez spécifier des utilisateurs membres du groupe Ventes ou des utilisateurs disposant de l'attribut de profil spécifique du poste Directeur commercial.

   Cliquez sur la flèche vers la gauche pour modifier une portion de règle préalablement spécifiée.

3. Cliquez sur OK.

4. Définition des conditions préalables pour le service (page 247)

Définition des conditions préalables pour le service

Dans l'onglet Conditions préalables, définissez les services dont les utilisateurs doivent disposer pour pouvoir demander ce service. Le service s'affiche dans la liste des services disponibles pour un utilisateur donné uniquement si cet utilisateur est membre de tous les services requis.

Si une durée est définie pour un service requis, cette durée s'applique alors au service que vous définissez. Par exemple, le service A est requis pour le service B. Le service A est associé à une durée d'une semaine. Le délai d'expiration du service B est également d'une semaine.

Procédez comme suit:

1. Dans l'onglet Conditions préalables, cliquez sur Ajouter un service.

   Une fenêtre de recherche apparaît.

2. Recherchez un service que vous voulez désigner comme condition préalable pour ce service.

   Pour afficher une liste de tous les services pour lesquels vous disposez de droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.

3. Sélectionnez un service et cliquez sur Sélectionner.

   Une liste mise à jour des conditions préalables pour ce service s'affiche.

Configuration de la notification par courriel du renouvellement de service

Certains services expirent au bout d'un certain temps.

Dans l'onglet Courriel, vous pouvez configurer une notification par courriel rappelant aux membres du service qu'ils doivent renouveler leur appartenance au service avant expiration. Les membres peuvent alors utiliser la tâche Renouveler la demande de service pour renouveler leur accès.

CA Cloud Access Manager fournit un modèle de courriel par défaut qui inclut du contenu dynamique. Ce contenu est automatiquement rempli lorsque le courriel est envoyé. Le contenu dynamique, qui apparaît entre crochets ({ }) dans l'éditeur de notification par courriel, ajoute un nom d'utilisateur spécifique, le nom du service et la date d'expiration dans le courriel.

Vous pouvez modifier le contenu de la notification par courriel dans l'éditeur. Par exemple, vous pouvez modifier le texte de l'objet ou du message, changer la police ou supprimer le contenu dynamique.

Notez les éléments suivants lors de la configuration des notifications par courriel :

- Si vous incluez du contenu dynamique dans la notification par courriel, ne modifiez pas le texte entre crochets ({ }).
- Si le service est associé à un service requis sur le point d'expirer, les notifications par courriel sont envoyées uniquement pour le service requis, même si les notifications par courriel sont configurées pour les deux services.

Procédez comme suit:

1. Dans l'onglet Courriel, activez la case à cocher Notification par courriel envoyée aux utilisateurs avant expiration d'un service pour activer les notifications.
2. (Facultatif) Personnalisez la notification par courriel à l'aide des contrôles dans l'éditeur.

   L'éditeur de notification par courriel prend en charge le format HTML. Vous pouvez ajouter du contenu HTML au message du courriel de notification en cliquant sur le bouton Basculer vers la source HTML (<>) dans la barre d'outils.
3. Description des actions d'exécution et de révocation (page 249)

Description des actions d'exécution et de révocation

Dans l'onglet Actions, vous définissez les droits et les informations (tâches, rôles, groupes et attributs) à ajouter, à modifier ou à supprimer lorsqu'un service est affecté ou retiré. Plus simplement, les actions de service définissent les actions réalisées par un service.

CA Cloud Access Manager utilise une stratégie Policy Xpress pour définir les conditions d'actions d'exécution et de révocation. CA Cloud Access Manager préconfigure cette stratégie pour que lorsqu'un utilisateur demande un service, les conditions et les données correctes existent. Le service est automatiquement exécuté ou retiré.

Un administrateur doit définir les actions du système pour l'exécution ou le retrait d'un service. Par exemple, lorsque vous créez un service, un administrateur peut spécifier que les membres du service reçoivent le rôle d'administration Directeur commercial, le rôle de provisionnement Salesforce.com et le groupe Ventes. De même, l'administrateur peut spécifier la suppression de ces droits lorsque le service est retiré.

Définition des actions d'exécution et de révocation pour le service

Dans l'onglet Actions, définissez les droits et les informations que le système ajoute, modifie, ou supprime lorsqu'un service est affecté ou supprimé pour un utilisateur.

Procédez comme suit:

1. Cliquez sur l'onglet Actions.

   La fenêtre Actions d'exécution/Actions de révocation s'affiche.

2. Cliquez sur Gérer les Actions d'exécution ou Gérer les Actions de révocation.

   La fenêtre Créer une stratégie Policy Xpress s'affiche.

   Les champs suivants sont prédéfinis pour la création d'une règle d'action :

   Nom

   Définit un nom convivial pour la règle d'action. Ce nom doit être unique.

   Description

   Détermine la signification de la règle d'action.

   Priorité

   Détermine la règle d'action qui s'exécute, si plusieurs sont respectées. Ce champ permet de définir les actions par défaut. Par exemple, si vous avez plusieurs règles, chacune pour un nom de service, il est possible de définir une valeur par défaut en ajoutant une règle supplémentaire sans condition mais avec une faible priorité (par exemple 10 si toutes les autres ont 5). Si aucune des règles de service sont respectées, le système utilise la valeur par défaut.

3. Sous Conditions d'une règle d'action, spécifiez des critères à respecter.
4. Sous Actions Ajouter, cliquez sur Ajouter une action en cas de correspondance.

   La fenêtre Ajouter une action en cas de correspondance s'affiche. Dans cette fenêtre, définissez les actions auxquelles le système procède en cas de correspondance de la règle.
5. Entrez un nom convivial définissant le but de l'action.

   Par exemple, entrez Ajouter le rôle d'administration pour le directeur commercial.
6. Sélectionnez la catégorie de l'action que le système doit effectuer.

   Par exemple, pour ajouter un rôle, sélectionnez la catégorie Rôles.
7. Sélectionnez le type d'action que le système doit effectuer.

   Par exemple, pour ajouter ou supprimer un rôle d'administration, sélectionnez le type Définir un rôle d'administration.
8. Sélectionnez la fonction que le système doit effectuer.

   Par exemple, pour ajouter un rôle d'administration, sélectionnez la fonction Ajouter.

   Remarque : Lorsque vous sélectionnez une fonction, une description de cette fonction s'affiche. Cette description permet de déterminer si la fonction sélectionnée fournit les résultats système recherchés.
9. Définissez l'action spécifique que le système doit effectuer.

   Par exemple, pour ajouter un rôle d'administration nommé Directeur commercial, entrez le nom du rôle ou cliquez sur le bouton Parcourir et sélectionnez Directeur commercial dans la liste des rôles d'administration disponibles.
10. Cliquez sur OK.

    Répétez cette procédure jusqu'à ce que toutes les actions souhaitées soient ajoutées pour ce service.
11. Cliquez sur OK.

    Le système associe les actions d'exécution et de révocation désignées au service. Lorsqu'un utilisateur reçoit le service, les droits associés et les informations sont ajoutés, modifiés ou supprimés.
12. Vous pouvez désormais affecter un service à un utilisateur (page 89).

Affectation d'un service à un utilisateur

Vous pouvez affecter un service directement à un utilisateur en particulier. Cet utilisateur devient *membre* du service.

Procédez comme suit:

1. A partir du menu de navigation, sélectionnez Services, Demander et afficher un accès.

   Une liste des services que vous pouvez administrer s'affiche.

2. Sélectionnez le service que vous voulez affecter à l'utilisateur, puis cliquez sur Sélectionner.

   Une liste d'utilisateurs affectés au service s'affiche.

3. Cliquez sur Demander l'accès.

4. Recherchez un utilisateur auquel vous voulez affecter le service.

   Pour afficher une liste de tous les utilisateurs pour lesquels vous avez des droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.

5. Sélectionnez un utilisateur et cliquez sur Sélectionner.

   Une liste mise à jour des utilisateurs affectés au service s'affiche.

6. Cliquez sur Enregistrer les modifications.

   L'utilisateur reçoit le service spécifié. L'utilisateur reçoit toutes les applications, tous les rôles, tous les groupes et tous les attributs associés au service.

Confirmation de l'affectation de services

Une fois que vous avez affecté un service à un utilisateur, confirmez que toutes les tâches associées au service sont terminées.

Procédez comme suit:

1. Dans le menu de navigation, sélectionnez Services, Afficher l'historique des demandes d'accès au service.

   Une fenêtre de recherche apparaît.

2. Recherchez le service que vous avez affecté à un utilisateur.

   Pour afficher une liste de tous les services pour lesquels vous disposez de droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.

   Une liste des services que vous pouvez administrer s'affiche.

3. Sélectionnez le service que vous avez affecté, et cliquez sur Sélectionner.

   Un historique d'actions associées au service s'affiche.

4. Cliquez sur Dernière modification pour afficher les actions les plus récentes en premier.
5. Confirmez que l'utilisateur a bien reçu le service.
6. Cliquez sur Fermer.

Disponibilité des services pour les utilisateurs

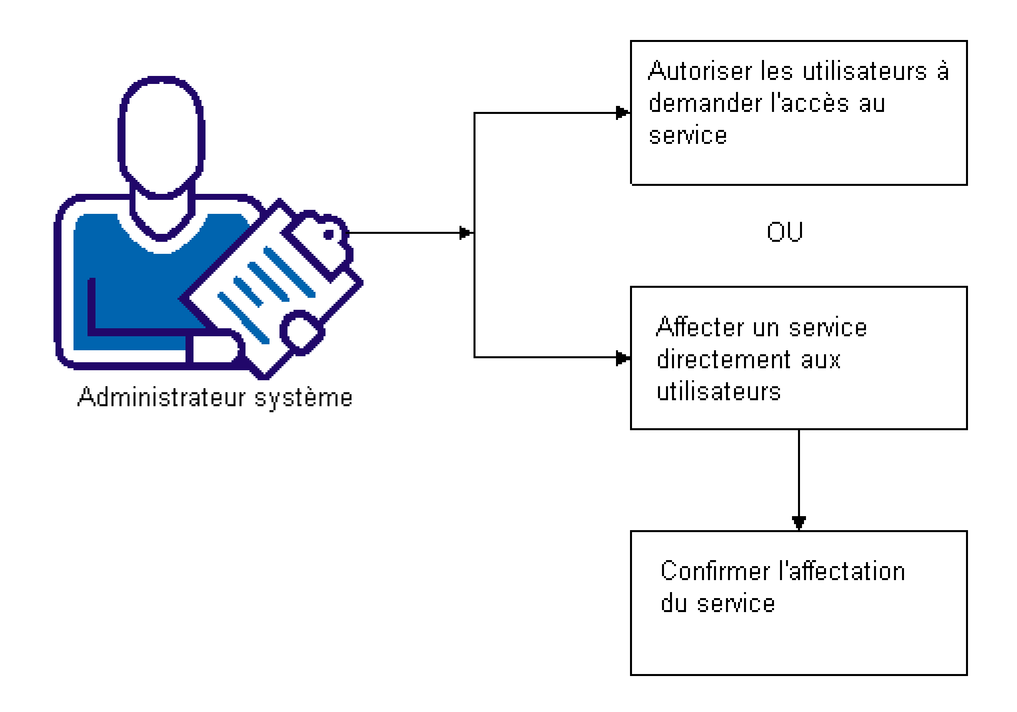
Les services simplifient la gestion des droits. Un service regroupe tous les droits dont un utilisateur a besoin pour un rôle donné. L'utilisateur peut accéder aux services par l'intermédiaire des tâches Demande d'accès, dans la console d'utilisateur. Les tâches Demande d'accès permettent à un utilisateur ou à un administrateur de demander, d'affecter, de retirer et de renouveler un service à travers l'interface utilisateur.

Les services permettent à un administrateur système de combiner des activités et des informations d'utilisateur (tâches, rôles, groupes et attributs) dans un package unique pour les gérer dans un ensemble. Par exemple, un nouvel employé des ventes a besoin d'un accès à un ensemble défini de tâches, de comptes sur des systèmes d'extrémité spécifiques et d'informations spécifiques ajoutées à son profil de compte d'utilisateur. Un administrateur système crée un service nommé Administration des ventes, contenant toutes les tâches, les rôles, les groupes et les informations d'attribut de profil requis pour un nouvel employé des ventes. Lorsqu'un administrateur affecte le service Administration des ventes à un utilisateur, cet utilisateur reçoit l'intégralité de l'ensemble des rôles, tâches, groupes et attributs de compte définis par le service.

Les utilisateurs peuvent également accéder aux services en effectuant eux-mêmes une demande d'accès. Dans la console d'utilisateur, chaque utilisateur dispose d'une liste des services disponibles qu'il peut demander. Cette liste contient les services définis sur Auto-abonnement par un administrateur système avec les droits appropriés, généralement pendant la création de service. A partir de la liste des services disponibles, les utilisateurs peuvent demander l'accès aux services dont ils ont besoin. Lorsque l'utilisateur demande l'accès à un service, la demande est exécutée automatiquement. Les tâches associées, les rôles, les groupes et les attributs sont affectés à l'utilisateur immédiatement. Un administrateur de CA Cloud Access Manager avec les droits appropriés peut également configurer l'exécution de services de sorte à requérir l'approbation de flux de travaux ou à générer des notifications par courriel.

Le schéma suivant affiche les informations nécessaires et les étapes à suivre pour rendre des services disponibles aux utilisateurs.

Mise à disposition des services aux utilisateurs



Vous pouvez rendre des services disponibles aux utilisateurs à l'aide des méthodes suivantes :

1. Autorisez les utilisateurs à demander eux-mêmes l'accès.

   Dans la console d'utilisateur de CA Cloud Access Manager, lorsque l'utilisateur clique sur Mon accès, puis sur Demander et afficher un accès, la liste des services disponibles qu'il peut demander s'affiche. Les services qui s'affichent dans cette liste sont définis sur Auto-abonnement par un administrateur de CA Cloud Access Manager avec les droits appropriés, généralement lors de la création des services.

   Lorsque l'utilisateur demande un accès, le système affecte le service à l'utilisateur. L'utilisateur reçoit toutes les applications, les rôles, les groupes et les attributs associés au service. Si le service inclut un rôle de lancement pour une application, une icône et un lien vers l'application s'affichent dans la page d'accueil de la console d'utilisateur.

2. Affectation d'un service directement à un utilisateur (page 89)

3. Si vous affectez un service directement à un utilisateur, confirmez l'affectation du service (page 254).

Affectation d'un service à un utilisateur

Vous pouvez affecter un service directement à un utilisateur en particulier. Cet utilisateur devient *membre* du service.

Procédez comme suit:

1. A partir du menu de navigation, sélectionnez Services, Demander et afficher un accès.

   Une liste des services que vous pouvez administrer s'affiche.

2. Sélectionnez le service que vous voulez affecter à l'utilisateur, puis cliquez sur Sélectionner.

   Une liste d'utilisateurs affectés au service s'affiche.

3. Cliquez sur Demander l'accès.

4. Recherchez un utilisateur auquel vous voulez affecter le service.

   Pour afficher une liste de tous les utilisateurs pour lesquels vous avez des droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.

5. Sélectionnez un utilisateur et cliquez sur Sélectionner.

   Une liste mise à jour des utilisateurs affectés au service s'affiche.

6. Cliquez sur Enregistrer les modifications.

   L'utilisateur reçoit le service spécifié. L'utilisateur reçoit toutes les applications, tous les rôles, tous les groupes et tous les attributs associés au service.

Confirmation de l'affectation de services

Une fois que vous avez affecté un service à un utilisateur, confirmez que toutes les tâches associées au service sont terminées.

Procédez comme suit:

1. Dans le menu de navigation, sélectionnez Services, Afficher l'historique des demandes d'accès au service.

   Une fenêtre de recherche apparaît.

2. Recherchez le service que vous avez affecté à un utilisateur.

   Pour afficher une liste de tous les services pour lesquels vous disposez de droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.

   Une liste des services que vous pouvez administrer s'affiche.

3. Sélectionnez le service que vous avez affecté, et cliquez sur Sélectionner.

   Un historique d'actions associées au service s'affiche.

4. Cliquez sur Dernière modification pour afficher les actions les plus récentes en premier.
5. Confirmez que l'utilisateur a bien reçu le service.
6. Cliquez sur Fermer.

Modification d'un service

En tant qu'administrateur système, vous pouvez modifier un service que vous avez créé préalablement. Par exemple, vous pouvez changer les droits que le service accorde aux membres des services en ajoutant un rôle au service. Vous pouvez également ajuster les règles d'administration et de propriété pour le service, les conditions requises pour les services et d'autres détails administratifs.

Si CA Cloud Access Manager a exécuté un service pour un utilisateur, les modifications apportées au service se seront pas envoyées à cet utilisateur. Si vous décidez de modifier un service, les utilisateurs ayant reçu le service avant les modifications disposeront des droits d'origine. Les utilisateurs qui reçoivent le service après les modifications disposeront des droits accordés par le service modifié. Exemple de scénario :

En tant qu'administrateur système, vous créez un service Directeur commercial qui octroie le rôle Directeur commercial et le groupe Ventes aux membres du service. Les utilisateurs demandent le service Directeur commercial et CA Cloud Access Manager exécute le service en accordant le rôle et le groupe appropriés aux utilisateurs. Vous décidez de modifier le service Directeur commercial pour inclure le rôle Responsable d'employés. Les membres existants du service ne reçoivent alors pas le rôle Responsable d'employés. Seuls les nouveaux membres du service Directeur commercial reçoivent ce rôle, en plus du rôle Directeur commercial et du groupe Ventes.

Vous pouvez alors modifier un service uniquement si le service ne comprend aucun membre. Modifiez un service uniquement si aucun utilisateur n'a demandé et reçu le service, et si aucun administrateur n'a affecté le service à un utilisateur.

Vous pouvez modifier des informations administratives, des règles de propriété et d'administration, des conditions de service et des droits (tâches, rôles, groupes et attributs) pour le service.

Procédez comme suit:

1. Connectez-vous à CA Cloud Access Manager avec un compte disposant de droits de gestion des services.

   Par exemple, le premier utilisateur d'un environnement dispose du rôle Gestionnaire de systèmes, qui comporte la tâche Modifier le service.

2. Dans le menu de navigation, sélectionnez Services.
3. Cliquez sur Gérer les services, puis sur Modifier le service.

   Une fenêtre de recherche apparaît.
4. Recherchez le service que vous voulez modifier.

   Pour afficher une liste de tous les services pour lesquels vous disposez de droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.
5. Sélectionnez un service et cliquez sur Sélectionner.

   Un message de confirmation apparaît.
6. Cliquez sur Oui.
7. Cliquez sur Soumettre.

   CA Cloud Access Manager applique vos modifications au service.

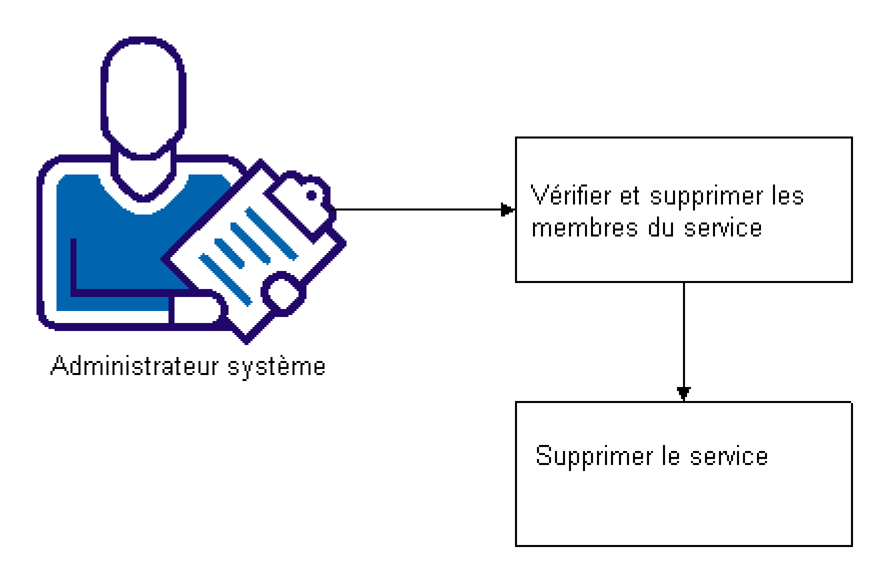
Chapitre 11: Suppression d'un service

En tant qu'administrateur système, vous pouvez supprimer un service. Un service supprimé est supprimé intégralement du système.

Si des utilisateurs sont affectés à un service, vous ne pouvez pas supprimer le service. Avant de supprimer un service, recherchez d'abord s'il contient des utilisateurs et supprimez les utilisateurs affectés, ou les *membres*.

Remarque : De même, si un utilisateur est membre d'un service, vous ne pouvez pas supprimer l'utilisateur. Supprimez d'abord le membre du service, puis supprimez l'utilisateur correspondant.

Le schéma suivant contient des informations importantes et les étapes à suivre pour supprimer un service.



Les rubriques suivantes décrivent la procédure de suppression d'un service :

1. Vérification et suppression de membres de service (page 258)
2. Suppression de service (page 258)

Vérification et suppression de membres de service

Avant de supprimer un service, recherchez d'abord s'il inclut des membres et supprimez-les.

Procédez comme suit:

1. Connectez-vous à CA Cloud Access Manager avec un compte disposant de droits de gestion des services.

   Par exemple, le premier utilisateur d'un environnement dispose du rôle Gestionnaire de systèmes, qui comporte la tâche Modifier le service.

2. Sélectionnez Services, Demander et afficher un accès.

   Une liste des services que vous pouvez administrer s'affiche.

3. Sélectionnez le service que vous voulez supprimer, puis cliquez sur Sélectionner.

   Une liste d'utilisateurs affectés au service s'affiche.

4. Si le service inclut des membres, désactivez les cases à cocher situées à côté des utilisateurs.
5. Cliquez sur Enregistrer les modifications.

   Un message de confirmation apparaît.

6. Cliquez sur Oui.

   CA Cloud Access Manager supprime les membres du service.

Suppression d'un service

Vous pouvez supprimer un service qui ne contient aucun membre de service.

Pour supprimer un service :

1. Connectez-vous à CA Cloud Access Manager avec un compte disposant de droits de gestion des services.

   Par exemple, le premier utilisateur d'un environnement dispose du rôle Gestionnaire de systèmes, qui comporte la tâche Supprimer un service.

2. Dans le menu de navigation, sélectionnez Services.
3. Cliquez sur Gérer les services, puis sur Supprimer un service.

   Une fenêtre de recherche apparaît.

4. Recherchez le service que vous voulez supprimer.

   Pour afficher une liste de tous les services pour lesquels vous disposez de droits d'administration, cliquez sur Rechercher sans modifier les critères de recherche.

5. Sélectionnez le service et cliquez sur Sélectionner.

   Un message de confirmation apparaît.

6. Cliquez sur Oui.

   Le service est supprimé.

Renouvellement de l'accès à un service

Certains services expirent après un certain temps. Les administrateurs peuvent renouveler un service pour les utilisateurs afin d'empêcher une interruption de l'accès.

Vous pouvez renouveler un service à l'aide des méthodes suivantes :

- Sélectionnez le service, puis sélectionnez l'accès utilisateur à renouveler.
- Sélectionnez l'utilisateur, puis le service à renouveler.

Remarque : Selon la configuration de l'environnement, l'utilisateur final peut également renouveler l'accès à l'aide de la tâche Renouveler l'accès.

La procédure suivante décrit la procédure de renouvellement de l'accès en sélectionnant d'abord le service. Si vous voulez sélectionner l'utilisateur d'abord, utilisez la tâches Demandes d'accès des utilisateurs, Gérer les demandes de renouvellement de l'utilisateur.

Procédez comme suit:

1. Cliquez sur Services, Renouveler l'accès dans la console d'utilisateur.
2. Recherchez et sélectionnez le service à renouveler.

   La console d'utilisateur affiche la liste des utilisateurs disposant actuellement de l'accès au service que vous avez sélectionné et la date d'expiration de leur accès.

3. Sélectionnez la durée pour le renouvellement dans la colonne Demande d'accès, puis cliquez sur OK.

   Les options dans le champ Durée sont définies une fois que le service est créé.

4. Cliquez sur Enregistrer les modifications.

Vous pouvez afficher le statut de renouvellement du service à l'aide de l'option Afficher l'historique des demandes d'accès au service dans la console d'utilisateur.

Chapitre 12: Synchronisation

Ce chapitre traite des sujets suivants :

Synchronisation des utilisateurs entre des serveurs

La configuration de la synchronisation dans CA Identity Manager permet d'assurer que les utilisateurs de l'annuaire d'entreprise et de l'annuaire de provisionnement disposent des données correspondantes. Pour gérer les changements apportés à l'un des annuaires, configurez les synchronisations entrante et sortante.

Synchronisation entrante

La synchronisation entrante assure la mise à jour des utilisateurs CA IdentityMinder avec les modifications apportées à l'annuaire de provisionnement. Ces modifications incluent celles appliquées à l'aide de systèmes comprenant des connecteurs au serveur de provisionnement. La synchronisation utilise les mappages définis dans la fenêtre Provisionnement de la console de gestion.

Basculement pour la synchronisation entrante

Le basculement vers une URL de serveur Identity Manager différente se produit uniquement si le serveur d'applications nommé par une URL n'est pas en cours d'exécution. Si le serveur d'applications est exécuté et accepte la notification, mais qu'il détecte ensuite une erreur de configuration, telle qu'un environnement inconnu ou non démarré, ce type d'erreurs bloque la remise de notifications. Pour le fonctionnement correct des notifications entrantes, ces problèmes doivent être résolus.

Synchronisation sortante

La synchronisation sortante implique l'utilisation de CA Identity Manager pour créer et mettre à jour des utilisateurs dans l'annuaire de provisionnement.

Création d'utilisateurs globaux à partir de CA Identity Manager

La création d'utilisateurs dans l'annuaire de provisionnement intervient uniquement pour provisionner des événements liés, tels que l'affectation d'un rôle de provisionnement à un utilisateur. Aucun utilisateur n'est créé dans l'annuaire de provisionnement si vous utilisez une tâche d'administration, sauf si cette tâche affecte un rôle ou inclut une stratégie d'identité qui affecte le rôle.

Lorsque la création d'utilisateurs dans CA Identity Manager déclenche la création d'utilisateurs dans l'annuaire de provisionnement, CA Identity Manager envoie un courriel contenant un mot de passe temporaire à l'adresse électronique du nouvel utilisateur tel que défini dans l'annuaire de provisionnement. L'utilisateur peut se connecter à la console d'utilisateurs à l'aide de ce mot de passe, qu'il devra alors modifier. Ainsi, le mot de passe est synchronisé entre le référentiel d'utilisateurs et l'annuaire de provisionnement.

Si l'utilisateur n'a aucune adresse électronique, il ne peut pas accéder à la console d'utilisateurs avant de changer le mot de passe dans le référentiel d'utilisateurs, ou avant qu'un administrateur CA IdentityMinder change son mot de passe dans le gestionnaire de provisionnement.

Remarque : Pour envoyer par courriel un mot de passe temporaire, les notifications par courriel doivent être activées pour l'environnement et l'événement CreateProvisioningUserNotificationEvent doit être configuré pour la notification par courriel. Reportez-vous au *Manuel de configuration*.

Mise à jour des utilisateurs globaux à l'aide de CA Identity Manager

Les mises à jour d'utilisateurs dans l'annuaire de provisionnement interviennent lorsque vous utilisez une tâche d'administration qui modifie des utilisateurs. Si aucun utilisateur global n'existe, aucune synchronisation ne se produira.

Les mappages de sortie établissent une correspondance entre les événements d'utilisateurs de CA Identity Manager et un événement de sortie qui affecte l'annuaire de provisionnement.

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

Si un utilisateur figure dans l'annuaire de provisionnement, mais non dans CA Identity Manager, vous pouvez le créer dans la console d'utilisateurs. Si vous avez mappé des attributs pour la tâche de création et que les utilisateurs ont le même ID, les attributs de l'utilisateur de provisionnement seront mis à jour dans l'annuaire de provisionnement. vous pouvez désormais gérer cet utilisateur dans CA Identity Manager.

Remarque : Si un événement met à jour des attributs d'utilisateur et que vous voulez synchroniser les valeurs avec CA IdentityMinder, vous devrez mapper les événements vers l'événement de sortie : POST_MODIFY_GLOBAL_USER.

Suppression d'utilisateurs globaux à l'aide de CA Identity Manager

Par défaut, la synchronisation sortante est configurée pour l'événement Supprimer un utilisateur. Lorsque vous supprimez un utilisateur dans CA Identity Manager, il est également supprimé de l'annuaire de provisionnement et de tous les comptes de terminal.

Si CA IdentityMinder ne peut pas supprimer le compte d'un utilisateur dans un terminal géré, il supprimera l'utilisateur des comptes restants, mais ne supprimera pas l'utilisateur de l'annuaire de provisionnement.

Par exemple, l'utilisateur A dispose d'un compte UNIX et d'un compte Exchange, gérés dans le serveur de provisionnement. Si l'utilisateur A est supprimé de CA Identity Manager, le serveur de provisionnement tentera de supprimer les comptes de cet utilisateur. Si le serveur de provisionnement ne peut pas supprimer le compte Exchange en raison d'une erreur de communication, il supprimera le compte UNIX de l'utilisateur A, mais ne supprimera pas l'utilisateur de l'annuaire de provisionnement. Toutefois, l'utilisateur A ne sera pas restauré dans le référentiel d'utilisateurs.

Activation de la synchronisation du mot de passe

Le serveur de provisionnement permet la synchronisation du mot de passe entre des utilisateurs de CA Identity Manager et les comptes d'utilisateurs de terminal associés. Deux configurations sont requises pour activer les modifications lancées par un terminal :

- Les terminaux doivent être configurés de sorte à capturer les modifications lancées par un terminal et les transmettre au serveur de provisionnement.

  Remarque : Pour plus d'informations sur la configuration des terminaux pour la synchronisation du mot de passe, reportez-vous au *Manuel d'administration de CA IdentityMinder*.

- L'attribut d'agent d'activation de la synchronisation du mot de passe doit être activé pour l'utilisateur global.

Pour activer la synchronisation de mots de passe :

1. Dans la console de gestion, sélectionnez Advanced Parameters (Paramètres avancés), Provisioning (Provisionnement).
2. Sous Endpoint Accounts, sélectionnez Enable Password Changes (Activer les modifications de mot de passe).
3. Cliquez sur Enregistrer.
4. Redémarrez le serveur d'applications.

Synchronisation des utilisateurs dans les tâches de création ou de modification d'utilisateurs

Dans l'onglet Profil d'une tâche de création ou de modification d'utilisateurs, les contrôles de synchronisation permettent d'assurer que les modifications apportées à CA Identity Manager sont également appliquées à l'utilisateur global. Si vous créez des tâches d'administration qui créent ou modifient des utilisateurs et que vous disposez de stratégies d'identité, définissez les contrôles de synchronisation comme suit :

- Définissez la synchronisation des utilisateurs sur A la fin de la tâche.
- Définissez la synchronisation des comptes sur A la fin de la tâche.

Remarque : Pour obtenir des résultats optimaux, sélectionnez A la fin de la tâche. Cependant, si vous sélectionnez l'option A la fin de la tâche pour une tâche incluant plusieurs événements, CA Identity Manager synchronisera les comptes à l'issue de tous les événements de la tâche. Si l'un de ces événements ou plusieurs requièrent une approbation de flux de travaux, cela peut prendre plusieurs jours. Pour que CA Identity Manager applique les stratégies d'identité ou synchronise les comptes avant la fin de tous les événements, sélectionnez l'option A chaque événement.

Si vous ajoutez des attributs à des tâches d'administration qui gèrent des utilisateurs, vous devez mettre à jour les mappages d'attributs dans la fenêtre Provisionnement de la console de gestion. Pour chaque attribut d'utilisateur dans CA Identity Manager, un attribut de provisionnement par défaut existe.

User Attribute	Provisioning Attribute
☐ %ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
☐ %EMAIL%	%EMAIL%
☐ %ENABLED_STATE%	%ENABLED_STATE%
☐ %FIRST_NAME%	%FIRST_NAME%
☐ %FULL_NAME%	%FULL_NAME%
☐ %IDENTITY_POLICY%	%IDENTITY_POLICY%
☐ %LAST_NAME%	%LAST_NAME%
☐ %PASSWORD%	%PASSWORD%
☐ %PASSWORD_DATA%	%PASSWORD_DATA%
☐ %USER_ID%	%USER_ID%

Tâches de synchronisation

Vous pouvez effectuer les types de synchronisation suivants :

Synchronisation des utilisateurs

Permet d'assurer que chaque utilisateur dispose des comptes nécessaires sur les terminaux gérés appropriés et que chaque compte est affecté aux modèles de compte appropriés à mesure qu'ils sont appelés par les rôles de provisionnement de l'utilisateur.

Synchronisation des comptes

Permet d'assurer que les valeurs d'attribut de capacité de comptes sont les valeurs appropriées, telles qu'indiquées par les modèles de compte affectés du compte. La synchronisation des comptes peut être forte ou faible. La synchronisation faible permet d'assurer que les attributs de capacité de compte disposent d'au moins la capacité minimum requise par ses modèles de compte. La synchronisation forte permet d'assurer que les attributs de capacité de compte disposent de la capacité exacte requise par ses modèles de compte. La synchronisation des comptes est forte si le compte appartient à au moins un modèle de compte dont la case à cocher Synchronisation forte est sélectionnée.

Aucune case à cocher Synchronisation forte correspondante ne régit la synchronisation des utilisateurs, mais un concept similaire existe. Lorsque vous émettez l'élément de menu Synchroniser l'utilisateur avec des rôles pour un utilisateur, deux options de synchronisation sont proposées :

- Ajout de comptes manquants et affectations de modèle de compte
- Suppression de comptes supplémentaires et affectations de modèle de compte
- La sélection unique de la case à cocher Ajouter, similaire à Synchronisation des comptes faible, indique que vous voulez que les utilisateurs globaux disposent au minimum de tous les comptes requis par leurs rôles de provisionnement affectés, mais que vous autorisez des utilisateurs à disposer de comptes supplémentaires non attribués par des rôles de provisionnement actuels.

Sélectionnez les cases à cocher Ajouter et Supprimer, similaire à Synchronisation de compte forte, de sorte que les rôles de provisionnement définissent exactement les comptes dont l'utilisateur doit disposer. Tout compte supplémentaire sera supprimé.

Choisissez Synchronisation des comptes faible/forte ou Synchronisation des utilisateurs faible/forte en fonction de la précision de la définition des rôles de provisionnement. Si vos utilisateurs correspondent à des rôles de provisionnement clairement définis, pour lesquels l'accès au compte est lié, utilisez la synchronisation forte.

Remarque : Certains types de terminal définissent la synchronisation forte comme valeur par défaut. Pour plus d'informations, consultez le manuel *Connectors Guide*.

La synchronisation des utilisateurs et la synchronisation des comptes sont des tâches distinctes que vous devez effectuer l'une après l'autre. En règle générale, vous effectuez d'abord la synchronisation des utilisateurs pour assurer que tous les comptes nécessaires sont créés, puis la synchronisation des comptes ultérieurement de sorte que le serveur de provisionnement affecte ou change les valeurs des attributs de compte.

Le serveur de provisionnement fournit deux ensembles d'options de menu de synchronisation pour les objets :

- Les options de menu de contrôle de synchronisation vérifient la synchronisation et renvoient une liste des comptes non conformes aux rôles de provisionnement ou aux modèles de compte.
- Les options de menu de synchronisation synchronisent les utilisateurs globaux avec leurs rôles de provisionnement ou leurs comptes avec leurs modèles de compte.

Si vous exécutez d'abord les fonctions de contrôle de synchronisation, le serveur de provisionnement indiquera les corrections qu'effectueront les fonctions de synchronisation. Si les fonctions de contrôle de synchronisation ne détectent aucun problème, les fonctions de synchronisation ne s'exécuteront pas.

Raison de la désynchronisation des utilisateurs

Voici quelques motifs de la désynchronisation des utilisateurs avec leurs rôles de provisionnement ou leurs modèles de compte :

- Les premières tentatives de création de comptes nécessaires ont échoué en raison de problèmes matériels ou logiciels dans votre réseau, entraînant la disparition de comptes.
- Les rôles de provisionnement et les modèles de compte ont peut-être été modifiés, entraînant la disparition ou la création de comptes supplémentaires.
- Les comptes ont été affectés aux modèles de comptes après leur création ; il existe donc des comptes non synchronisés avec leurs modèles de compte.
- La création d'un compte est retardée, car le compte a été défini pour être créé plus tard.
- Un nouveau terminal a été acquis. Lors de l'exploration et de la corrélation, le serveur de provisionnement n'affecte aucun rôle de provisionnement aux utilisateurs de manière automatique ; vous devez donc mettre à jour le rôle de sorte à indiquer les utilisateurs devant posséder des comptes sur le nouveau terminal. Un compte corrélé avec un utilisateur est répertorié comme compte supplémentaire lorsque l'utilisateur est synchronisé.
- Un compte existant a été affecté à un utilisateur en le copiant vers celui-ci ; une corrélation manuelle a donc été exécutée et un compte supplémentaire a été établi.
- Un compte a été créé pour un utilisateur autrement qu'en affectant l'utilisateur à un rôle. Par exemple, si vous copiez un utilisateur vers un modèle de compte inclus dans aucun de ses rôles de provisionnement, ce compte sera répertorié comme compte supplémentaire ou comme compte avec un modèle de compte supplémentaire. Si vous copiez l'utilisateur vers un terminal pour créer un compte à l'aide du modèle de compte par défaut du terminal, il peut s'agit d'un compte supplémentaire.

Synchronisation des utilisateurs

La synchronisation des utilisateurs crée, met à jour ou supprime des comptes de sorte à les rendre conformes au rôle de provisionnement affecté à un utilisateur. Ainsi, si les administrateurs ajoutent ou suppriment des comptes sur votre terminal géré à l'aide d'outils natifs et que vous n'avez pas relancé d'exploration récente de votre terminal pour mettre à jour l'annuaire de provisionnement, il se peut que la synchronisation des utilisateurs indique qu'aucun problème n'est survenu, alors qu'un utilisateur peut constater la présence de comptes supplémentaires ou l'absence de comptes.

Synchronisation d'utilisateurs avec des rôles

Vous pouvez vérifier la synchronisation sur des utilisateurs afin de répertorier des comptes supplémentaires ou des modèles de compte et des comptes manquants. Lorsque vous sollicitez la synchronisation d'un utilisateur avec des rôles, le serveur de provisionnement vérifie que cet utilisateur dispose de tous les comptes requis par ses rôles de provisionnement et que chaque compte appartienne aux modèles de compte corrects.

- Pour cette tâche, vous pouvez sélectionner une case à cocher pour créer le compte sur le terminal. Si plusieurs modèles de compte utilisent le même compte dans les rôles de provisionnement de l'utilisateur, le compte sera créé en fusionnant tous les modèles de compte pertinents.
- Pendant la synchronisation d'un utilisateur avec des rôles, vous pouvez supprimer des comptes supplémentaires. Vous pouvez également déterminer que vos utilisateurs nécessitent d'autres comptes que ceux requis par leurs rôles de provisionnement. Dans ce cas, ne sélectionnez pas l'option Supprimer.

  Si un compte supprimé réside dans un terminal géré pour lequel les suppressions de comptes ont été désactivées, ce compte ne sera pas supprimé.

Création de comptes

Les rôles de provisionnement contenant des modèles de compte associés à des terminaux, un utilisateur doit disposer de comptes répertoriés sur chaque terminal avec les attributs de compte corrects.

Pour cette tâche, vous pouvez sélectionner une case à cocher pour créer le compte sur le terminal. Si plusieurs modèles de compte utilisent le même compte dans les rôles de provisionnement de l'utilisateur, le compte sera créé en fusionnant tous les modèles de compte pertinents.

Ce compte est affecté aux modèles de compte qui ne sont actuellement pas synchronisés avec le compte. La synchronisation de compte n'est pas nécessaire pour les nouveaux comptes.

Suppression de comptes

Pendant la synchronisation d'un utilisateur avec des rôles, vous pouvez supprimer des comptes supplémentaires. Vous pouvez également déterminer que vos utilisateurs nécessitent d'autres comptes que ceux requis par leurs rôles de provisionnement. Dans ce cas, ne sélectionnez pas l'option Supprimer.

Si un compte supprimé réside dans un terminal géré pour lequel les suppressions de comptes ont été désactivées, ce compte ne sera pas supprimé.

Ajout de modèles de compte à des comptes

Si une ou plusieurs affectations de modèle de compte sont manquantes pour un compte, la synchronisation de l'utilisateur avec des modèles de compte affectera un compte existant à ces modèles de compte. Si un compte est affecté à un ou plusieurs nouveaux modèles de compte, la synchronisation de compte sera automatiquement exécutée pour mettre à jour les attributs de capacité du compte avec les fonctions spécifiées par les modèles de compte.

Après sa mise à jour à partir de la synchronisation de l'utilisateur avec des modèles de compte, le compte peut être synchronisé ou non avec ses modèles de compte. Si l'un des modèles de compte ajoutés était un modèle de compte de synchronisation forte ou si deux ou plusieurs modèles de compte ont été ajoutés à un compte, la synchronisation de l'utilisateur avec des rôles lancera une synchronisation de compte complète sur le compte. Toutefois, si un seul modèle de compte de synchronisation faible a été ajouté, la synchronisation de l'utilisateur avec les modèles de compte lancera une synchronisation de compte impliquant uniquement ce modèle de compte. Si le compte n'était pas préalablement inclus dans la synchronisation de compte avec ses autres modèles de compte avant cette mise à jour, il se peut qu'il ne soit toujours pas inclus dans la synchronisation de compte par la suite.

Suppression de modèles de compte à partir de comptes

La synchronisation d'un utilisateur avec des rôles permet également de supprimer des modèles de compte supplémentaires d'un compte. Pour cela, l'option Supprimer doit être sélectionnée. Lorsque la synchronisation des utilisateurs détermine qu'un compte doit être mis à jour pour supprimer un ou plusieurs modèles de compte supplémentaires, la synchronisation des comptes est automatiquement exécutée sur le compte pour synchroniser ses attributs de capacité avec les modèles de compte restant sur le compte.

Cette synchronisation des comptes qui intervient lors de la suppression des modèles de compte d'un compte sera forte si l'un des modèles de compte restants est marqué pour la synchronisation forte et faible si tous les modèles de compte restants sont marqués pour la synchronisation faible.

L'utilisation de la synchronisation faible ou forte affecte la suppression des capacités de compte octroyées antérieurement lorsqu'un modèle de compte affecté à un compte est ultérieurement supprimé. Avec la synchronisation forte, une capacité accordée par un modèle de compte, telle que l'appartenance à un groupe ou un quota supérieur, sera supprimée (l'appartenance au groupe supprimée ou le quota diminué) si aucun des modèles de compte restants sur le compte n'attribue cette capacité. Toutefois, avec la synchronisation faible, le compte reste en général inchangé, car le serveur de provisionnement ne différencie pas les capacités supplémentaires à la demande et les capacités accordées à travers des modèles de compte.

Certains attributs de capacité à valeurs multiples désignés comme attributs SyncRemoveValues font exception à cette règle. Un attribut simple à valeurs multiples représentant une collecte de valeurs affectées au compte (une liste d'appartenance au groupe, par exemple), sera généralement répertorié comme attribut SyncRemoveValues. Pour ces attributs, l'action de synchronisation faible qui intervient lors de la suppression d'un modèle de compte à partir d'un compte supprimera des valeurs attribuées par le modèle de compte qui est supprimé, à condition que ces valeurs ne soient pas elles-mêmes attribuées par l'un des modèles de compte restants.

Par exemple, si vous créez vos modèles de compte de sorte que chacun d'eux affecte une appartenance à un groupe unique à votre compte, la fonctionnalité SyncRemoveValues impliquera que, lors de la modification des rôles de provisionnement d'un utilisateur global de sorte à ce qu'un modèle de compte particulier ne lui soit plus nécessaire, le compte sera mis à jour pour ne plus appartenir au groupe attribué par ce modèle de compte. Vous remarquerez que cela n'est pas exactement identique à la synchronisation forte, car les appartenances de groupe attribuées à des comptes au-delà des attributions aux modèles de compte sont conservées.

Pour tous les attributs à valeur unique et certains attributs à valeurs multiples non désignés comme attributs SyncRemoveValues, l'action de synchronisation faible lors de la suppression d'un modèle de compte à partir d'un compte est identique à l'action de synchronisation faible normale : les capacités ne sont jamais supprimées.

Si vous voulez que les capacités ne soient jamais supprimées par la synchronisation faible, désactivez la fonctionnalité SyncRemoveValues en définissant le paramètre de configuration de domaine de synchronisation/suppression des valeurs de modèle de compte des comptes sur Non.

Synchronisation du modèle de compte

Les modifications que vous apportez aux modèles de comptes affectent les comptes existants de la façon suivante :

- Si vous modifiez la valeur d'un attribut de capacité, l'attribut de compte correspondant est mis à jour, le cas échéant, afin d'être synchronisé avec la valeur d'attribut de modèle de compte. Reportez-vous à la description des synchronisations faible et forte.
- Certains attributs de compte sont conçus par le connecteur pour ne pas être mis à jour lors des modifications de modèle de compte. Par exemple, certains attributs que le type de terminal permet uniquement de définir pendant la création de compte et l'attribut Mot de passe.

Synchronisation des attributs de capacité

Lorsque vous modifiez les attributs de capacité d'un modèle de compte, l'attribut correspondant des comptes peut changer. L'impact sur les attributs d'un compte dépend de deux facteurs.

- Si le modèle de compte est défini pour utiliser une synchronisation faible ou forte
- Si le compte appartient à plusieurs modèles de compte

Synchronisation faible

La *synchronisation faible* garantit que les utilisateurs disposent des attributs de capacité minimum requis pour leurs comptes. La synchronisation faible est la valeur par défaut de la plupart des types de terminaux. Si vous mettez à jour un modèle qui utilise la synchronisation faible, CA IdentityMinder met à jour les attributs de capacité comme suit :

- Si un champ Numéro est mis à jour dans un modèle de compte et que le nouveau numéro est supérieur au numéro figurant dans le compte, CA IdentityMinder modifie la valeur du compte de manière à ce qu'elle corresponde au nouveau numéro.
- Si une case à cocher auparavant désactivée dans un modèle de compte est activée ultérieurement, CA IdentityMinder met à jour la case à cocher sur les comptes sur lesquels elle est désactivée.
- Si une liste est modifiée dans un modèle de compte, CA IdentityMinder met à jour tous les comptes pour inclure toutes les valeurs de la nouvelle liste qui n'étaient pas incluses dans la liste de valeurs du compte.

Si un compte appartient à d'autres modèles de compte (utilisant la synchronisation faible ou forte), CA IdentityMinder consulte uniquement le modèle en cours de modification. Cette action est plus efficace que la vérification de chaque modèle de compte. Dans la mesure où la synchronisation faible n'ajoute que des fonctionnalités aux comptes, il n'est généralement pas nécessaire de consulter ces autres modèles de compte.

Remarque : Lors de la propagation à partir d'un modèle de compte à synchronisation faible, il se peut que des modifications qui suppriment ou réduisent les fonctionnalités ne soient pas synchronisées vers certains comptes. N'oubliez pas que les fonctionnalités ne sont jamais supprimées ni réduites dans le cadre de la synchronisation faible. La propagation ne tient pas compte des autres modèles de comptes et des résultats de la synchronisation faible.

Dans cette situation, utilisez la synchronisation d'utilisateurs avec les modèles de compte pour synchroniser le compte avec ses modèles de compte.

Synchronisation forte

La synchronisation forte assure que les comptes incluent les mêmes attributs de compte que les attributs spécifiés dans le modèle de compte.

Par exemple, si vous ajoutez un groupe à un modèle de compte UNIX existant. Auparavant, le modèle de compte créait des membres de comptes du groupe Personnel. Désormais, vous voulez créer les membres de comptes des deux groupes Personnel et Système. Tous les comptes associés au modèle de compte sont synchronisés lorsque chaque compte devient membre des groupes Personnel et Système (et aucun autre groupe). Un compte n'appartenant pas au groupe Personnel est ajouté aux deux groupes.

Autres facteurs dont vous devez tenir compte :

- Si le modèle de compte utilise la synchronisation forte, les comptes appartenant à des groupes, autre que Personnel et Système, sont supprimés de ces autres groupes.
- Si le modèle de compte utilise la synchronisation faible, les comptes sont ajoutés aux groupes Personnel et Système. Les comptes pour lesquels d'autres groupes sont définis restent membres de ces groupes.

Remarque : Si vous n'appliquez pas les modifications aux comptes chaque fois que vous mettez à jour les attributs de capacité d'un modèle de compte, vous devez synchroniser régulièrement vos comptes avec leurs modèles de compte pour garantir la synchronisation des comptes avec leurs modèles.

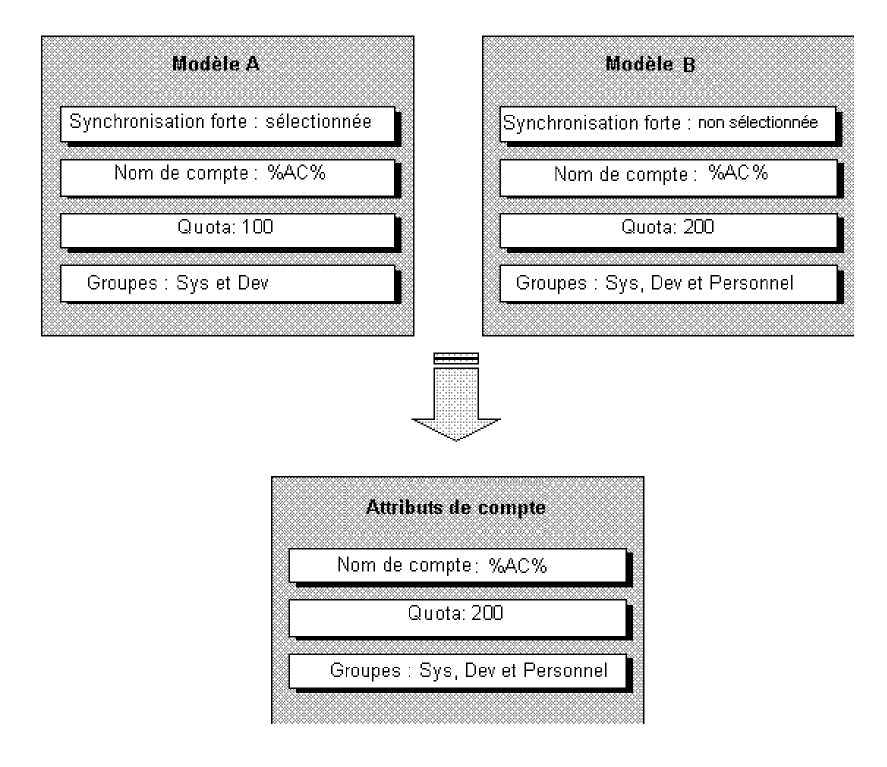
Comptes avec plusieurs modèles

La synchronisation dépend également de l'appartenance du compte à plusieurs modèles de compte. Si un compte inclut uniquement un modèle de compte et que ce modèle utilise la synchronisation forte, chaque attribut est mis à jour pour correspondre exactement à la valeur d'attribut du modèle de compte. Le résultat est le même qu'avec un attribut initial.

Un compte peut appartenir à plusieurs modèles de compte : c'est le cas lorsqu'un utilisateur global appartient à plusieurs rôles de provisionnement pour lesquels un même niveau d'accès est attribué sur le même terminal géré. Dans ce cas, CA IdentityMinder combine ces modèles de compte en un modèle de compte applicable qui attribut le sur-ensemble des fonctionnalités à partir des modèles de compte individuels. Ce modèle de compte utilise la synchronisation faible si tous ses modèles de compte individuels sont faibles ou la synchronisation forte si un des modèles de compte individuels est fort.

Remarque : Vous utilisez généralement uniquement la synchronisation faible ou uniquement la synchronisation forte pour les modèles de compte qui contrôlent un compte, si les rôles de votre société définissent intégralement les accès dont vos utilisateurs ont besoin. Si vos utilisateurs ne correspondent à aucun rôle clair et que vous ayez besoin de flexibilité pour attribuer des fonctionnalités supplémentaires aux comptes d'utilisateur, utilisez la synchronisation faible. Si vous êtes en mesure de définir des rôles pour spécifier exactement les accès dont vos utilisateurs ont besoin, utilisez la synchronisation forte.

L'exemple suivant décrit la combinaison de plusieurs modèles de compte en un modèle de compte unique applicable. Dans cet exemple, un modèle de compte est marqué pour la synchronisation faible et l'autre pour la synchronisation forte. Par conséquent, le modèle de compte applicable combinant les deux modèles de compte est considéré comme un modèle de compte de synchronisation forte. L'attribut Quota de nombre entier accepte la valeur la plus grande des deux modèles de compte et l'attribut Groupes à valeurs multiples accepte l'union des valeurs des deux stratégies.



Attributs uniquement pour les nouveaux comptes

Dans un modèle de compte, certains attributs sont uniquement appliqués lorsque vous créez un compte. Par exemple, l'attribut Mot de passe est un expression de règle qui définit le mot de passe pour les nouveaux comptes. Cette expression de règle ne met jamais à jour le mot de passe d'un compte. Les modifications apportées à l'expression de règle de mot de passe ont un impact uniquement sur les comptes créés après la définition de l'expression de règle.

De même, une expression de règle de modèle pour un attribut de compte en lecture seule affecte uniquement les comptes créés après la définition de l'expression de règle. Sa modification n'a aucun effet sur les comptes existants.

Synchronisation des comptes

La synchronisation des comptes met à jour les attributs de capacité afin d'assurer que le compte dispose des capacités spécifiées par les modèles de compte. Cela n'affecte pas les attributs initiaux du compte.

Pour synchroniser des modifications apportées aux attributs de capacité dans un modèle de compte avec ses comptes, utilisez l'une des options de menu de synchronisation décrites dans cette section.

Vérification de la synchronisation des comptes

Vous pouvez vérifier la synchronisation des comptes pour les terminaux et les utilisateurs. Cette action renvoie une liste de comptes non conformes aux modèles de compte. Le tableau suivant décrit les événements qui surviennent lorsque vous vérifiez la synchronisation des comptes sur chaque objet :

Objet	Synchronise
Terminal	les attributs de compte pour chaque compte sur un terminal et assure leur conformité aux modèles de compte associés.
Utilisateur global	les attributs de compte pour chaque compte d'un utilisateur et assure leur conformité aux modèles de compte associés.

Synchronisation des comptes

Vous pouvez effectuer la synchronisation des comptes sur des terminaux, des utilisateurs et des modèles de compte. Le tableau suivant répertorie l'effet de la synchronisation des comptes sur chaque objet :

Objet	Synchronise
Terminal	chaque compte sur un terminal avec ses modèles de compte associés.
Utilisateur global	chaque compte d'un utilisateur global avec chaque modèle de compte associé.

Chapitre 13: Stratégies d'identité

Ce chapitre traite des sujets suivants :

Stratégies d'identité

Une stratégie d'identité désigne un ensemble de modifications métiers qui ont lieu lorsqu'un utilisateur satisfait à une certaine condition ou règle. Vous pouvez utiliser des ensembles de stratégies d'identité aux fins suivantes.

- Automatiser certaines tâches de gestion d'identité, telles que l'affectation de rôles, d'appartenances à un groupe ou de ressources, ou encore la modification d'attributs de profils d'utilisateurs).
- Appliquer la séparation des fonctions. Par exemple, vous pouvez créer un ensemble de stratégies d'identité qui interdit aux membres du rôle Signataire de chèque de disposer du rôle Approbateur de chèque et empêche quiconque dans l'entreprise de rédiger un chèque supérieur à 10 000 euros.
- Appliquer la conformité. Par exemple, vous pouvez effectuer un audit sur les utilisateurs disposant d'un certain titre et générant plus de 100 000 euros.

  Les stratégies d'identité qui appliquent la conformité sont nommées *stratégies de conformité*.

Les modifications métiers associées à une stratégie d'identité sont notamment les suivantes.

- L'affectation ou le retrait de rôles, y compris des rôles de provisionnement (uniquement si vous utilisez un annuaire de provisionnement).
- L'affectation ou le retrait d'une appartenance à un groupe.
- La mise à jour d'attributs dans un profil d'utilisateur.

Par exemple, une entreprise peut créer une stratégie d'identité selon laquelle tous les vice-présidents appartiennent au groupe Membre du Country Club et disposent du rôle Approbateur de salaire. Lorsque le titre d'un utilisateur est redéfini sur Vice-président et que cet utilisateur est synchronisé avec la stratégie d'identité, CA IdentityMinder ajoute l'utilisateur au groupe et au rôle appropriés. Lorsqu'un vice-président est promu PDG, il ne remplit plus la condition spécifiée par la stratégie d'identité Vice-président. Les modifications apportées par cette stratégie sont donc révoquées et les nouvelles modifications basées sur la stratégie PDG sont appliquées.

Les actions de modification qui se produisent en fonction d'une stratégie d'identité contiennent des événements pouvant être placés sous le contrôle du flux de travaux et faire l'objet d'un audit. Dans l'exemple précédent, le rôle Approbateur de salaire accorde des droits significatifs à ses membres. Pour protéger le rôle Approbateur de salaire, l'entreprise peut créer un processus de flux de travaux qui nécessite un ensemble d'approbations avant l'affectation du rôle et configurer CA IdentityMinder pour effectuer l'audit de l'affectation du rôle.

Pour simplifier la gestion des stratégies d'identité, celles-ci sont regroupées dans un ensemble. Par exemple, les stratégies Vice-président et PDG peuvent appartenir à l'ensemble de stratégies d'identité Droits des cadres.

Remarque : CA IdentityMinder inclut un autre type de stratégie d'identité, appelé *stratégie d'identité préventive* (page 299). Ces stratégies, qui s'exécutent avant la soumission d'une tâche, permettent à un administrateur de contrôler les violations de stratégie avant d'affecter des droits ou de modifier des attributs de profil. Si une violation se produit, l'administrateur peut l'effacer avant de soumettre la tâche.

Feuille de calcul de planification d'ensembles de stratégies d'identité

Un ensemble de stratégies d'identité contient une ou plusieurs stratégies d'identité. Avant de créer un ensemble de stratégies d'identité, utilisez la feuille de calcul suivante pour planifier chaque stratégie d'identité de l'ensemble.

Question	Votre réponse
Quel nom souhaitez-vous affecter à la stratégie d'identité ?	
A quels utilisateurs la stratégie d'identité s'applique-t-elle ?	
Lorsqu'une stratégie d'identité est appliquée à un utilisateur, quelles actions CA IdentityMinder doit-il effectuer ?	
Lorsqu'une stratégie d'identité qui s'appliquait à un utilisateur n'est plus applicable, quelles actions CA IdentityMinder doit-il effectuer ?	
CA IdentityMinder doit-il appliquer les modifications dans une stratégie d'identité plusieurs fois ou uniquement la première fois qu'un utilisateur remplit les conditions spécifiées par la stratégie ?	

Une fois cette feuille de calcul remplie pour chaque stratégie d'identité de votre ensemble, vérifiez que les stratégies n'entrent pas en conflit avec d'autres stratégies. Par exemple, vérifiez qu'une stratégie n'accorde pas un droit qu'une autre stratégie révoque.

Création d'un ensemble de stratégies d'identité

Pour créer un ensemble de stratégies d'identité, vous devez disposer du rôle Gestionnaire de systèmes ou d'un rôle incluant la tâche Créer un ensemble de stratégies d'identité.

Pour créer un ensemble de stratégies d'identité, effectuez les étapes suivantes :

1. Définition du profil de l'ensemble de stratégies d'identité (page 279)
2. Création d'une règle de membre de l'ensemble de stratégies (page 280)
3. Création d'un ensemble de stratégies d'identité (page 280)
4. Spécification des propriétaires de l'ensemble de stratégies d'identité (page 290)

Remarque : Pour utiliser les stratégies pour un environnement CA IdentityMinder, activez les stratégies d'identité dans la console de gestion CA IdentityMinder. Pour plus d'informations, voir le *Manuel de configuration*.

Définition du profil de l'ensemble de stratégies d'identité

L'onglet Profil permet de définir les propriétés de base d'un ensemble de stratégies d'identité.

Pour définir le profil d'un ensemble de stratégies d'identité

1. Sélectionnez Stratégies, Gérer les stratégies d'identité, Créer un ensemble de stratégies d'identité dans la console d'utilisateur.

   Vous devez être connecté à CA IdentityMinder en tant qu'utilisateur disposant de droits pour gérer les stratégies d'identité. Le rôle Gestionnaire système par défaut inclut ces droits.

2. Choisissez de créer un nouvel ensemble de stratégies d'identité ou de créer une copie d'un ensemble existant.
3. Entrez le nom de l'ensemble de stratégies d'identité.
4. Entrez la catégorie de l'ensemble de stratégies d'identité.

   La catégorie regroupe les ensembles de stratégies d'identité ayant des objectifs similaires pour la génération de rapports. Le champ Catégorie est obligatoire.

5. Si vous le souhaitez, entrez une description de l'ensemble de stratégies d'identité.
6. Si vous ne souhaitez pas que l'ensemble de stratégies d'identité soit utilisable, désactivez la case à cocher Activé.
7. Une fois l'onglet Profil complété, sélectionnez l'onglet Stratégies afin de créer les stratégies pour l'ensemble de stratégies d'identité.

Informations complémentaires :

Création d'une règle de membre de l'ensemble de stratégies (page 280)
Création d'une stratégie d'identité (page 280)

Création d'une règle de membre de l'ensemble de stratégies

Vous pouvez créer une règle de membre pour un ensemble de stratégies afin que l'ensemble de stratégies ne s'applique qu'à certains utilisateurs. La règle est évaluée avant l'évaluation des stratégies d'identité incluses dans l'ensemble, ce qui permet de bénéficier d'un gain de temps significatif. Par exemple, si la règle de membre limite l'évaluation de la stratégie d'identité à 10 % des utilisateurs, elle permet d'économiser 90 % du temps d'évaluation.

Pour créer une règle de membre de l'ensemble de stratégies :

1. Cliquez sur l'onglet Stratégies.
2. Cliquez sur le symbole Modifier sous Règle du membre de l'ensemble de stratégies.
3. Entrez une règle pour appliquer la stratégie à certains utilisateurs uniquement.
4. Cliquez sur OK.

Informations complémentaires :

Création d'une stratégie d'identité (page 280)

Création d'une stratégie d'identité

Une fois le profil et la règle de membre de l'ensemble de stratégies d'identité définis, vous pouvez définir les stratégies d'identité de cet ensemble.

Remarque : Dans les implémentations à grande échelle, l'évaluation des règles de stratégies d'identité peut prendre beaucoup de temps. Pour réduire le temps d'évaluation des règles comprenant des attributs d'utilisateur, vous pouvez activer l'option d'évaluation en mémoire. Pour plus d'informations, voir le *Manuel de configuration*.

Pour créer une stratégie d'identité :

1. Cliquez sur l'onglet Stratégies.
2. Cliquez sur Ajouter.
3. Entrez le nom de la stratégie d'identité.
4. Cochez la case Appliquer une fois si vous voulez appliquer la stratégie uniquement lorsqu'un utilisateur correspond pour la première fois à la stratégie.

5. Cochez la case Conformité pour marquer cette stratégie en tant que stratégie de conformité.

   Ceci entraîne les actions ci-après.

   - CA IdentityMinder peut générer des rapports pour les utilisateurs qui ne sont pas synchronisés avec les stratégies de conformité.
   - L'action Violation de la conformité s'affiche dans la zone de liste Action lors de l'application/la suppression de la stratégie.

6. Dans la section Condition de stratégie, identifiez les utilisateurs auxquels la stratégie s'applique.
7. Dans la section Action lors de l'application de la stratégie, définissez les actions que CA IdentityMinder effectue lorsque la stratégie d'identité est appliquée à un utilisateur.
8. Dans la section Action lors de la suppression de la stratégie, définissez les actions que CA IdentityMinder effectue lorsqu'un utilisateur ne remplit plus les conditions définies dans la stratégie d'identité.
9. Cliquez sur OK.

Remarque : Pour utiliser l'ensemble de stratégies d'identité que vous avez créé, activez les stratégies d'identité dans la console de gestion. Pour plus d'informations, voir le *Manuel de configuration*.

Paramètre Appliquer une fois

CA IdentityMinder applique les stratégies d'identité différemment, en fonction du paramètre Appliquer une fois.

Paramètre Appliquer une fois

Si le paramètre Appliquer une fois est activé, CA IdentityMinder applique les modifications associées à la stratégie d'identité lorsqu'un utilisateur remplit *pour la première fois* les conditions définies dans la stratégie. Les actions de modification associées à la stratégie ne sont effectuées qu'une seule fois. Par conséquent, CA IdentityMinder n'applique pas les mises à jour de la stratégie aux utilisateurs si la stratégie a précédemment été appliquée.

Lorsqu'un utilisateur ne remplit plus les conditions définies dans la stratégie, CA IdentityMinder effectue les actions de suppression de la stratégie.

Le paramètre Appliquer une fois est généralement utilisé lors du provisionnement de ressources. Par exemple, vous pouvez disposer d'une stratégie qui affecte un téléphone portable aux gestionnaires. Lorsqu'un utilisateur devient pour la première fois un gestionnaire, il reçoit un téléphone portable. CA IdentityMinder n'affecte le téléphone portable qu'une seule fois, et non pas chaque fois que la stratégie est évaluée. Si la stratégie de téléphone portable est mise à jour pour inclure un modèle de téléphone portable plus récent, CA IdentityMinder n'affecte pas le nouveau modèle aux gestionnaires existants.

Remarque : Le provisionnement de ressources est disponible lorsque CA IdentityMinder est intégré à un serveur de provisionnement.

Paramètre Appliquer une fois

Si le paramètre Appliquer une fois n'est pas activé, les actions de modification associées à la stratégie d'identité sont effectuées chaque fois que la stratégie d'identité est évaluée. Cela signifie que CA IdentityMinder effectue les actions de modification pour chaque utilisateur qui remplit les conditions définies dans la stratégie, que ces actions aient été précédemment appliquées ou non.

En général, vous désactivez le paramètre Appliquer une fois dans une stratégie d'identité qui applique la conformité. Par exemple, vous pouvez créer une stratégie d'identité qui limite la capacité de dépense des gestionnaires à 5 000 dollars. Si CA IdentityMinder rencontre un gestionnaire dont la capacité de dépense est définie sur 10 000 dollars, il redéfinit cette capacité sur 5 000. Chaque fois qu'un gestionnaire est synchronisé avec la stratégie d'identité, CA IdentityMinder vérifie que la capacité de dépense est définie correctement.

Si une modification manuelle rentrant en conflit avec une action de modification est apportée à un profil d'utilisateur, CA IdentityMinder écrase la modification lorsque l'utilisateur est synchronisé avec la stratégie.

Dans l'exemple précédent, si quelqu'un augmente manuellement la capacité de dépense d'un gestionnaire à 10 000 dollars, CA IdentityMinder redéfinit la capacité de dépense sur 5 000 dollars lorsque le gestionnaire est synchronisé avec la stratégie.

Le tableau suivant récapitule les effets liés à l'activation ou à la désactivation du paramètre Appliquer une fois.

Si Appliquer une fois est...	**Alors...**
Activé(e)	■ Les actions de modification associées à la stratégie d'identité ne sont effectuées qu'une seule fois. ■ Les modifications manuelles apportées après application de la stratégie d'identité sont conservées. ■ Les mises à jour ne sont pas appliquées aux utilisateurs qui remplissent les conditions définies dans une stratégie d'identité si CA IdentityMinder a précédemment appliqué la stratégie. ■ Lorsqu'un utilisateur ne remplit plus les conditions définies dans une stratégie d'identité, CA IdentityMinder effectue les actions de suppression.
Désactivé	■ Les actions de modification associées à la stratégie d'identité sont effectuées chaque fois qu'un utilisateur est synchronisé avec la stratégie. ■ Les modifications manuelles sont écrasées lorsque la stratégie d'identité est appliquée. ■ Les mises à jour de la stratégie sont appliquées lorsqu'un utilisateur est synchronisé. ■ Lorsqu'un utilisateur ne remplit plus les conditions définies dans une stratégie d'identité, CA IdentityMinder effectue les actions de suppression.

Conditions de stratégies

Les conditions de stratégies sont les règles qui déterminent l'ensemble des utilisateurs auxquels une stratégie d'identité s'applique.

Les options disponibles sont décrites dans le tableau ci-dessous.

Syntaxe	**Condition**	**Exemple**
(Tout)	La stratégie d'identité s'applique à tous les utilisateurs.	
où <filtre-utilisateur>	L'utilisateur doit correspondre à une ou plusieurs valeurs d'attributs.	Utilisateurs dont titre=gestionnaire et localité=est

Syntaxe	Condition	Exemple
dans <règle-org>	L'utilisateur doit appartenir à des organisations nommées. **Remarque :** Lorsque vous sélectionnez cette option, CA IdentityMinder affiche une nouvelle zone de liste dans laquelle vous pouvez sélectionner les options suivantes. ■ organisation <organisation> [et moins que] : utilisez une fenêtre de recherche d'organisations pour sélectionner une organisation et, le cas échéant, inclure les organisations enfants de cette dernière. ■ Organisations où <filtre-organisation> [et moins que] : spécifiez un filtre pour sélectionner une ou plusieurs organisations.	Utilisateurs dans l'organisation Ventes et moins que
où <filtre-utilisateur> et figurant dans <règle-org>	L'utilisateur doit correspondre à des attributs d'utilisateur spécifiques et appartenir à une organisation donnée.	titre=gestionnaire et organisation=Ventes*
membres de <règle-membre-groupe>	L'utilisateur doit appartenir à un groupe qui satisfait à une condition spécifiée par les attributs du groupe. **Remarque :** Lorsque vous sélectionnez cette option, CA IdentityMinder affiche une nouvelle zone de liste dans laquelle vous pouvez sélectionner les options suivantes. ■ groupe <groupe> : utilisez une fenêtre de recherche de groupes pour sélectionner un groupe. ■ groupe où <filtre-groupe> : spécifiez un filtre qui sélectionne un ou plusieurs groupes.	Utilisateurs membres de groupes où propriétaire=PDG

Syntaxe	Condition	Exemple
membres de <règle-rôle>	L'utilisateur doit être membre d'un rôle. Il peut s'agir des rôles suivants. ■ Un rôle d'accès ■ Un rôle d'administration ■ Un rôle de provisionnement **Remarque :** Pour utiliser des rôles de provisionnement, CA IdentityMinder doit être intégré à un serveur de provisionnement. Pour plus d'informations, reportez-vous au *manuel d'installation*.	Utilisateurs membres du rôle Centre d'assistance
qui sont administrateurs de <règle-rôle>	L'utilisateur doit être administrateur d'un rôle. Il peut s'agir des rôles suivants. ■ Un rôle d'accès ■ Un rôle d'administration ■ Un rôle de provisionnement **Remarque :** Pour utiliser des rôles de provisionnement, CA IdentityMinder doit être intégré à un serveur de provisionnement. Pour plus d'informations, reportez-vous au *manuel d'installation*.	Utilisateurs qui sont administrateurs du rôle Gestionnaire des ventes
qui sont propriétaires de <règle-rôle>	L'utilisateur doit être propriétaire d'un rôle. Il peut s'agir des rôles suivants. ■ Un rôle d'accès ■ Un rôle d'administration ■ Un rôle de provisionnement **Remarque :** Pour utiliser des rôles de provisionnement, CA IdentityMinder doit être intégré à un serveur de provisionnement. Pour plus d'informations, reportez-vous au *manuel d'installation*.	Utilisateurs qui sont propriétaires du rôle Gestionnaire d'utilisateurs
renvoyés par la requête <requête-LDAP>	L'utilisateur doit satisfaire à une condition basée sur une requête LDAP.	Utilisateur satisfaisant aux conditions d'une requête LDAP. Par exemple : (departmentNumber=Comptes)

Syntaxe	Condition	Exemple
dans <contrainte-union-administration>	L'utilisateur doit remplir au moins l'une des conditions spécifiées dans une liste de conditions. Vous pouvez inclure, dans une contrainte d'union d'administration, les types de filtres suivants. ■ Membre de rôle d'accès/d'administration/de provisionnement ■ Administrateur de rôle d'accès/d'administration/de provisionnement ■ Propriétaire de rôle d'accès/d'administration/de provisionnement ■ Membre d'un groupe	Utilisateurs membres *ou* propriétaires du rôle Gestionnaire de certifications
dans <contrainte-intersection-administrative>	L'utilisateur doit remplir toutes les conditions spécifiées dans une liste de conditions. Vous pouvez inclure, dans une contrainte d'union d'administration, les types de filtres suivants. ■ Membre de rôle d'accès/d'administration/de provisionnement ■ Administrateur de rôle d'accès/d'administration/de provisionnement ■ Propriétaire de rôle d'accès/d'administration/de provisionnement ■ Membre d'un groupe	Utilisateurs membres des rôles Auteur de contrat *et* Approbateur de contrat

Actions lors de l'application/la suppression de stratégies

Vous pouvez définir les actions de modification que CA IdentityMinder effectue lorsqu'il évalue la stratégie d'identité. Il s'agit des actions suivantes.

Actions lors de l'application de la stratégie

Un ensemble d'actions que CA IdentityMinder effectue lorsqu'un utilisateur remplit les conditions spécifiées par la stratégie.

Actions lors de la suppression de la stratégie

Un ensemble d'actions que CA IdentityMinder effectue lorsqu'un utilisateur ne remplit plus les conditions spécifiées par la stratégie.

Les actions que CA IdentityMinder peut effectuer lorsque des stratégies d'identité sont appliquées ou supprimées sont les mêmes. Pour plus d'informations, reportez-vous au tableau suivant.

Action de modification	Description
Ajouter au groupe <nom-groupe> [...]	Ajoute des utilisateurs à un groupe. Lorsque vous sélectionnez cette option, CA IdentityMinder affiche une fenêtre dans laquelle vous pouvez rechercher le groupe de votre choix.
Ajouter à <nom-groupe> dans l'organisation de l'utilisateur	Ajoute des utilisateurs à un groupe local. Lorsque vous sélectionnez cette option, CA IdentityMinder affiche une zone de texte dans laquelle vous pouvez entrer le nom du groupe de votre choix.
Définir <attribut-utilisateur-valeur-unique> sur valeur	Définit la valeur d'un attribut dans un profil d'utilisateur. S'il existe une valeur, CA IdentityMinder la remplace par la valeur spécifiée dans l'action de modification.
Ajouter <valeur> à <attribut-utilisateur-valeurs-multiples>	Ajoute une valeur à un attribut d'utilisateur à valeurs multiples. Cette option n'écrase pas les valeurs existantes.
Promouvoir en tant que membre du rôle d'accès	Affecte les utilisateurs à un rôle d'accès.
Promouvoir en tant qu'administrateur du rôle d'accès	Transforme les utilisateurs en administrateurs d'un rôle d'accès.
Promouvoir en tant que membre du rôle d'administration	Transforme les utilisateurs en membres d'un rôle d'administration.
Promouvoir en tant qu'administrateur du rôle d'administration	Transforme les utilisateurs en administrateurs d'un rôle d'administration.
Promouvoir en tant que membre du rôle de provisionnement	Transforme les utilisateurs en membres d'un rôle de provisionnement, ce qui crée des comptes de terminaux associés. **Remarque :** Pour utiliser des rôles de provisionnement, CA IdentityMinder doit être intégré à un serveur de provisionnement. Reportez-vous au *manuel d'installation* de votre serveur d'applications.
Promouvoir en tant qu'administrateur du rôle de provisionnement	Transforme les utilisateurs en administrateurs d'un rôle de provisionnement. **Remarque :** Pour utiliser des rôles de provisionnement, CA IdentityMinder doit être intégré à un serveur de provisionnement. Reportez-vous au *manuel d'installation* de votre serveur d'applications.

Action de modification	Description
Supprimer du groupe <nom-groupe> [...]	Supprime des utilisateurs d'un groupe. Lorsque vous sélectionnez cette option, CA IdentityMinder affiche une fenêtre dans laquelle vous pouvez rechercher le groupe de votre choix.
Supprimer de <nom-groupe> dans l'organisation de l'utilisateur	Supprime des utilisateurs d'un groupe local. Lorsque vous sélectionnez cette option, CA IdentityMinder affiche une zone de texte dans laquelle vous pouvez entrer le nom du groupe de votre choix.
Supprimer <valeur> de <attribut-utilisateur-valeurs-multiples>	Supprime une valeur d'un attribut d'utilisateur à valeurs multiples.
Supprimer le membre du rôle d'accès	Retire un rôle d'accès.
Supprimer l'administrateur du rôle d'accès	Retire les droits d'administrateur pour un rôle d'accès spécifique.
Supprimer le membre du rôle d'administration	Retire un rôle d'administration.
Supprimer l'administrateur du rôle d'administration	Retire les droits d'administrateur pour un rôle administration spécifique
Supprimer le membre du rôle de provisionnement	Retire un rôle de provisionnement.
Supprimer l'administrateur du rôle de provisionnement	Retire les droits d'administrateur pour un rôle de provisionnement spécifique.
Envoyer un message d'audit	Envoie un message que vous créez à la base de données d'audit. Ce message peut apparaître dans un rapport que vous créez.
Violation de la conformité	Envoie un message que vous créez à la base de données d'audit. Si vous créez un rapport de conformité, le message apparaît chaque fois que la stratégie d'identité est appliquée à un utilisateur ou supprimée de ce dernier. Pour plus d'informations sur l'audit, reportez-vous au *manuel de configuration*. **Remarque :** Pour utiliser l'option Violation de la conformité, vous devez activer la case à cocher Conformité de l'onglet Profil de l'ensemble de stratégies d'identité.

Action de modification	Description
Accepter (Action lors de l'application de stratégies uniquement)	Autorise la soumission de la tâche en cas de violation de la stratégie d'identité préventive. Lorsque vous sélectionnez cette action, vous fournissez un message que CA IdentityMinder consigne dans la base de données d'audit et affiche dans Afficher les tâches soumises en cas de violation.
Rejeter (Action lors de l'application de stratégies uniquement)	Empêche la soumission d'une tâche en cas de violation d'une stratégie d'identité. Cette action est utilisée avec les stratégies d'identité préventives pour éviter que des utilisateurs ne reçoivent des droits susceptibles d'entraîner des conflits d'intérêts ou une fraude. Lorsque vous sélectionnez cette action, vous spécifiez également un message que CA IdentityMinder affiche en cas de violation. Le message est stocké dans la base de données d'audit et apparaît dans la console d'utilisateur.
Avertissement (Action lors de l'application de stratégies uniquement)	Déclenche un processus de flux de travaux en cas de violation d'une stratégie d'identité préventive, si vous associez cette violation à une stratégie d'approbation de flux de travaux. CA IdentityMinder autorise la soumission de la tâche, que le flux de travaux soit configuré ou non. **Remarque :** Pour plus d'informations sur l'association d'un processus de flux de travaux à une stratégie d'identité préventive, reportez-vous à la rubrique Flux de travaux et stratégies d'identité préventives. (page 305) Lorsque vous sélectionnez cette action, vous spécifiez également un message que CA IdentityMinder affiche en cas de violation. Le message est stocké dans la base de données d'audit et apparaît dans Afficher les tâches soumises.

Informations complémentaires :

Stratégies d'identité préventives (page 299)
Flux de travaux et stratégies d'identité préventives (page 305)

Spécification des propriétaires de l'ensemble de stratégies d'identité

Dans l'onglet Propriétaires, vous définissez des règles qui déterminent quelles personnes peuvent être propriétaires de l'ensemble de stratégies d'identité. Un propriétaire d'ensemble de stratégies d'identité peut modifier les informations de base relatives à l'ensemble et peut ajouter, modifier ou supprimer des stratégies d'identité dans l'ensemble.

Pour remplir l'onglet Propriétaires :

1. Définissez des règles de propriété, qui déterminent quels utilisateurs peuvent modifier le rôle.
2. Cliquez sur Soumettre.

Création d'un ensemble de stratégies d'identité

CA IdentityMinder inclut les tâches suivantes permettant de gérer un ensemble de stratégies d'identité :

- Afficher l'ensemble des stratégies d'identité
- Modifier un ensemble des stratégies d'identité
- Supprimer l'ensemble de stratégies d'identité

Par défaut, lorsqu'un administrateur utilise l'une de ces tâches, CA IdentityMinder affiche la liste de tous les ensembles de stratégies d'identité dont cet administrateur est propriétaire. L'administrateur peut alors choisir dans la liste l'ensemble de stratégies d'identité dont il a besoin.

Dans un environnement Identity Manager incluant de nombreux ensembles de stratégies d'identité, vous pouvez personnaliser les tâches d'affichage, de modification et de suppression d'ensembles de stratégies d'identité afin que les administrateurs puissent rechercher un ensemble de stratégies d'identité au lieu d'afficher les ensembles dans une liste.

Pour personnaliser ces tâches :

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Rôles d'administration, puis Modifier la tâche d'administration.

   La fenêtre Modifier la tâche d'administration s'ouvre.
2. Recherchez et sélectionnez la tâche à personnaliser.
3. Dans l'onglet Portée, sélectionnez Tous les ensembles de stratégies d'identité.

   Lorsque vous sélectionnez cette option, CA IdentityMinder utilise la définition de fenêtre Recherche d'un ensemble de stratégies d'identité par défaut.
4. Cliquez sur Soumettre.

Synchronisation des utilisateurs et des stratégies d'identité

Lorsque vous utilisez des stratégies d'identité, il est important que vous compreniez l'évaluation des stratégies par CA IdentityMinder et leur application aux utilisateurs. Si vous ne comprenez pas parfaitement le processus de synchronisation des utilisateurs, vous risquez de configurer des ensembles de stratégies d'identité qui génèrent des résultats indésirables.

La procédure suivante décrit l'évaluation et l'application des stratégies d'identité par CA IdentityMinder.

1. Le processus de synchronisation des utilisateurs commence :
   - **Automatiquement** : vous pouvez configurer des tâches CA IdentityMinder pour déclencher automatiquement la synchronisation des utilisateurs.
   - **Manuellement** : la tâche de synchronisation de l'utilisateur de la console d'utilisateur permet de synchroniser un utilisateur.
2. CA IdentityMinder détermine l'ensemble de stratégies d'identité qui s'applique à un utilisateur.
3. CA IdentityMinder compare cet ensemble à la liste des stratégies qui ont déjà été appliquées à cet utilisateur.

   Remarque : La liste des stratégies ayant été appliquées à un utilisateur est stockée dans l'attribut %IDENTITY_POLICY% du profil de l'utilisateur. Pour obtenir des informations sur la configuration de cet attribut, reportez-vous au *manuel de configuration*.

   - Si une stratégie d'identité figure dans la liste des stratégies applicables *et* qu'elle n'a *pas* déjà été appliquée à l'utilisateur, CA IdentityMinder l'ajoute à une liste d'affectation.
   - Si une stratégie d'identité figure dans la liste des stratégies applicables, qu'elle a déjà été appliquée à l'utilisateur et que son paramètre Appliquer une fois est désactivé, CA IdentityMinder l'ajoute à la liste de réaffectation.
   - Si une stratégie d'identité ne figure pas dans la liste des stratégies applicables, qu'elle a déjà été appliquée à l'utilisateur et que ce dernier ne remplit plus les conditions de cette stratégie, CA IdentityMinder ajoute cette stratégie à une liste de désaffectation.
4. Une fois que CA IdentityMinder a évalué toutes les stratégies d'un utilisateur, il les applique dans l'ordre suivant.

   a. Stratégies d'identité de la liste de désaffectation

   b. Stratégies d'identité de la liste d'affectation

   c. Stratégies d'identité de la liste de réaffectation

5. Une fois les stratégies d'identité appliquées, CA IdentityMinder les réévalue pour savoir si des modifications supplémentaires sont requises, selon les modifications apportées au cours du premier processus de synchronisation (étapes 2 à 4).

   Cette étape vise à vérifier que les modifications apportées en appliquant les stratégies d'identité n'ont pas déclenché d'autres stratégies d'identité.

6. CA IdentityMinder continue à réévaluer et à appliquer les stratégies d'identité jusqu'à ce que l'utilisateur soit synchronisé avec toutes les stratégies applicables ou jusqu'à ce que CA IdentityMinder atteigne le niveau de traitement récursif maximum, défini dans la console de gestion.

   Par exemple, une stratégie d'identité peut modifier un département d'utilisateur lorsque qu'un rôle est affecté à ce dernier. Le nouveau département déclenche une autre stratégie d'identité. Cependant, si le niveau de récursion est défini sur 1, la modification suivante n'est pas effectuée tant que l'utilisateur n'a pas été synchronisé à nouveau.

   Pour plus d'informations sur la définition du niveau de récursion, reportez-vous à l'Aide en ligne de la console de gestion.

Configuration de la synchronisation automatique des utilisateurs

CA IdentityMinder peut automatiquement synchroniser les comptes d'utilisateurs avec les stratégies d'identité à différents stades du cycle de vie d'une tâche.

Une tâche CA IdentityMinder génère des *événements*, qui sont des activités détectables se produisant pendant le traitement des tâches. Par exemple, la tâche Créer un utilisateur génère les événements CreateUserEvent, AddUserToGroupEvent et AssignAccessRoleEvent. Vous pouvez configurer CA IdentityMinder afin qu'il synchronise les utilisateurs une fois une tâche ou un événement terminé.

Remarque : La section Synchroniser des utilisateurs avec des stratégies d'identité (page 291) fournit plus d'informations sur le processus de synchronisation des utilisateurs.

Pour configurer une tâche afin de déclencher la synchronisation des utilisateurs :

1. Connectez-vous à CA IdentityMinder en tant qu'utilisateur autorisé à modifier des tâches d'administration.

2. Sélectionnez Rôles et tâches, Tâches d'administration, puis Modifier la tâche d'administration.

   CA IdentityMinder affiche une fenêtre de recherche.

3. Recherchez et sélectionnez la tâche d'administration allant déclencher la synchronisation des utilisateurs.

4. Dans le champ Synchronisation des utilisateurs de l'onglet Profil de la tâche, sélectionnez l'une des options suivantes :

   ■ **Désactivé** : cette tâche ne déclenche pas la synchronisation des utilisateurs.

   ■ **A la fin de la tache** : CA IdentityMinder démarre le processus de synchronisation des utilisateurs une fois tous les événements terminés. Ce paramètre est l'option de synchronisation par défaut des tâches Créer un utilisateur, Modifier un utilisateur et Supprimer un utilisateur. Le paramètre par défaut de toutes les autres tâches est Désactivé.

     Remarque : Si vous activez l'option A la fin de la tâche pour une tâche incluant plusieurs événements, CA IdentityMinder synchronise les utilisateurs uniquement lorsque tous les événements de la tâche sont terminés. Si l'un ou plusieurs de ces événements requièrent une approbation de flux de travaux, cela peut prendre plusieurs jours. Pour que CA IdentityMinder applique les stratégies d'identité avant la fin de tous les événements, activez l'option A chaque événement.

   ■ **A chaque événement** : CA IdentityMinder démarre le processus de synchronisation des utilisateurs lorsque chaque événement d'une tâche est terminé.

     Dans le cas des tâches comportant un événement principal et secondaire pour le même utilisateur, si vous définissez la synchronisation des utilisateurs sur A chaque événement, vous risquez d'obtenir plus d'évaluations pour lesquelles des stratégies s'appliquent à un utilisateur que si vous sélectionnez l'option A la fin de la tâche.

Synchronisation manuelle des utilisateurs

Vous pouvez synchroniser manuellement un utilisateur avec un ensemble de stratégies d'identité pour vous assurer qu'un compte d'utilisateur dispose des droits adéquats ou satisfait une stratégie de conformité.

Vous pouvez synchroniser un utilisateur manuellement à l'aide de la tâche Synchroniser l'utilisateur de la console d'utilisateur CA IdentityMinder.

Remarque : Pour que la tâche Synchroniser l'utilisateur fonctionne correctement, l'option Synchroniser l'utilisateur doit être définie sur Désactivé et l'option Synchronisation de compte sur A la fin de la tâche ou A chaque événement. Pour obtenir de meilleures performances, choisissez l'option A la fin de la tâche. Pour définir ces options, accédez à l'onglet Profil de la tâche Synchroniser l'utilisateur.

La tâche Synchroniser l'utilisateur comporte les onglets ci-après.

- **Stratégies correspondantes** : affiche la liste des stratégies d'identité que CA IdentityMinder applique à l'utilisateur lorsque la tâche Synchroniser l'utilisateur est soumise.

  Remarque : L'onglet Stratégies correspondantes n'affiche que les stratégies d'identité qui s'appliquent à l'utilisateur au moment où vous accédez à la tâche Synchroniser l'utilisateur. Lorsque l'utilisateur est synchronisé avec ces stratégies, des modifications peuvent se produire et déclencher d'autres stratégies d'identité. Pour que CA IdentityMinder n'applique pas les nouvelles stratégies jusqu'à ce que vous les examiniez, définissez le niveau de traitement récursif des ensembles de stratégies d'identité sur 1 dans la console de gestion CA IdentityMinder. Une fois la tâche Synchroniser l'utilisateur soumise, accédez-y de nouveau pour examiner les stratégies.

- **Stratégies déjà appliquées** : affiche la liste des stratégies d'identité ayant déjà été appliquées à l'utilisateur.
- **Résumé de la synchronisation** : affiche toutes les stratégies d'identité qui s'appliquent à l'utilisateur et les actions de modification de ces stratégies.

Pour synchroniser un compte d'utilisateur :

1. Connectez-vous à Identity Manager en tant qu'utilisateur autorisé à utiliser la tâche Synchroniser l'utilisateur. Par défaut, les utilisateurs disposant du rôle Gestionnaire de systèmes peuvent utiliser cette tâche.
2. Sélectionnez Stratégies, puis Synchroniser l'utilisateur.

   La tâche Synchroniser l'utilisateur apparaît.
3. Sélectionnez l'onglet Résumé de la synchronisation.
4. Examinez les stratégies et les actions associées que CA IdentityMinder appliquera à l'utilisateur, puis cliquez sur Soumettre.

Vérification de la synchronisation des utilisateurs

Pour vérifier que les modifications appropriées sont effectuées lorsqu'un utilisateur est synchronisé avec des stratégies d'identité, examinez l'onglet Stratégies déjà appliquées de la tâche Synchroniser l'utilisateur.

1. Connectez-vous à CA IdentityMinder en tant qu'utilisateur autorisé à utiliser la tâche Synchroniser l'utilisateur. Par défaut, les utilisateurs disposant du rôle Gestionnaire de systèmes peuvent utiliser cette tâche.
2. Sélectionnez Stratégies, puis Synchroniser l'utilisateur.

   La tâche Synchroniser l'utilisateur apparaît.
3. Sélectionnez l'onglet Stratégies déjà appliquées.
4. Examinez les stratégies et les actions associées que CA IdentityMinder a appliqué à l'utilisateur.

Ensembles de stratégies d'identité dans un environnement Identity Manager

Les sections suivantes décrivent différentes manières d'utiliser les stratégies d'identité :

- Exemple : spécification automatique d'attributs d'utilisateurs (page 295)
- Exemple : affectation de ressources et de droits (page 296)
- Exemple : application de la conformité (page 297)
- Exemple : application de la séparation des fonctions (page 297)

Exemple : Spécification automatique d'attributs d'utilisateurs

Vous pouvez utiliser un ensemble de stratégies d'identité pour affecter automatiquement des valeurs d'attributs d'utilisateurs en fonction d'une autre valeur d'attribut ou d'un autre droit d'utilisateur. Par exemple, vous pouvez créer un ensemble de stratégies d'identité qui indique automatiquement l'adresse postale d'un utilisateur en fonction de son bureau à domicile.

Pour configurer un ensemble de stratégies d'identité pour des adresses d'employés, créez une stratégie d'identité comportant les paramètres ci-après pour chaque emplacement de bureau.

Paramètre	**Valeur**
Condition de stratégie	office = <emplacement_bureau>
Action lors de l'application de la stratégie	set Street Address = <une_adresse> set City = <une_ville> Set State/Province = <un_état ou une_province> Set Postal Code = <un_code_postal>

La figure suivante présente des exemples de stratégies figurant dans l'ensemble de stratégies d'identité Adresses d'employés.

Stratégies d'identité

Ensemble de stratégies

	Nom de la stratégie	Règle du membre de stratégie	Action lors de l'application de la stratégie
	NY	où (Office = "NY")	Définir Address sur 601 rue Définir City sur NY Définir State sur NY Définir Postal code sur 10017
	Boston	où (Office = "Boston")	Définir Address sur 201 rue Définir City sur Boston Définir State sur MA Définir Postal code sur 02451

Exemple : Affectation de ressources et de droits

Les stratégies d'identité peuvent affecter automatiquement des ressources (par exemple, des comptes de domaines) ou accorder des droits (par exemple, transformer un utilisateur en un membre d'un rôle) lorsque les utilisateurs remplissent les conditions de la stratégie. Par exemple, vous pouvez créer un ensemble de stratégies d'identité qui affectent des ressources et des rôles en fonction du titre d'un utilisateur.

Pour créer un ensemble de stratégies d'identité afin d'affecter des ressources et des rôles, créez une stratégie d'identité comportant les paramètres ci-après pour chacun des titres existant dans votre organisation.

Paramètre	Valeur
Condition de stratégie	title = <un_titre>
Action lors de l'application de la stratégie	Des actions qui affectent des ressources ou des droits aux utilisateurs remplissant les conditions de la stratégie, par exemple : ■ promouvoir en tant que membre de <un_groupe> ■ promouvoir en tant que membre du rôle d'administration <un_rôle_d_administration> ■ promouvoir en tant que membre du rôle de provisionnement <un_rôle_de_provisionnement>
Action lors de la suppression de la stratégie	Des actions qui suppriment les ressources ou les droits lorsqu'un utilisateur ne remplit plus les conditions de la stratégie. Par exemple, si Identity Manager a transformé l'utilisateur en membre d'un rôle lorsque la stratégie d'identité a été appliquée, vous pouvez configurer Identity Manager pour révoquer le rôle lorsque l'utilisateur ne remplit plus les conditions de la stratégie.

La figure suivante présente des exemples de stratégies figurant dans l'ensemble de stratégies d'identité Ressources d'employés.

Stratégies d'identité

Ensemble de stratégies

	Nom de la stratégie	Règle du membre de stratégie	Action lors de l'application de la stratégie	Action lors de la suppression de la stratégie
	Directeur	où (Title = "Directeur")	Promouvoir en tant que membre du rôle d'administration UM Promouvoir en tant que membre du rôle de provisionnement UP	Supprimer le membre du rôle d'administration UM
	HR	où (Title = "HR")	Promouvoir en tant que membre du rôle d'administration UM Ajouter au groupe UG Promouvoir en tant que membre du rôle de provisionnement UP	Supprimer du groupe UG Supprimer le membre du rôle d'administration UM Supprimer le membre du rôle de provisionnement UP

Exemple : Application de la conformité

Vous pouvez configurer des stratégies d'identité pour définir des conditions qui doivent ou ne doivent pas exister et effectuer certaines actions en fonction de l'évaluation de ces conditions. Par exemple, vous pouvez définir une stratégie de conformité selon laquelle la limite de dépense des gestionnaires doit être de 5 000 dollars. Si la limite de dépense d'un gestionnaire atteint 10 000 dollars, CA IdentityMinder peut réinitialiser sa limite et enregistrer une violation de conformité à des fins d'audit.

Pour créer un ensemble de stratégies de conformité afin d'appliquer des limites de dépense, créez une stratégie d'identité comportant les paramètres ci-après.

Paramètre	**Valeur**
Appliquer une fois	Non activé
Conformité	Activé(e)
Condition de stratégie	Conditions qui définissent la conformité ou une violation de conformité ; par exemple : title=<un_titre> AND Spending Limit > <une_limite_de_dépense>
Action lors de l'application de la stratégie	Actions que CA IdentityMinder doit effectuer lorsque les conditions de stratégie s'appliquent ; par exemple : ■ Message de violation de conformité : limite de dépense dépassée ■ Définir la limite de dépense sur <une_valeur>

La figure suivante présente la stratégie de conformité décrite dans cet exemple.

Stratégies d'identité

Ensemble de stratégies

	Nom de la stratégie	Règle du membre de stratégie	Action lors de l'application de la stratégie
	Gestionnaires	où (Title = "Gestionnaire" et Spending limit > "5000")	Message de violation de la conformité : Limite de dépenses dépasse pas 5000

Exemple : Application de la séparation des fonctions

Les stratégies d'identité peuvent définir des rôles mutuellement exclusifs et ne pouvant pas être accordés simultanément au même utilisateur. Par exemple, vous pouvez empêcher un gestionnaire d'utilisateurs pouvant accorder des augmentations d'être également un approbateur de salaire.

Pour créer un ensemble de stratégies d'identité qui applique la séparation des fonctions, créez une stratégie d'identité comportant les paramètres ci-après.

Paramètre	Valeur
Appliquer une fois	Non activé
Conformité	Activé
Condition de stratégie	Utilisez l'option "dans <contrainte-intersection-administrative>" pour définir un ensemble de conditions qui violent une stratégie métier. Si un utilisateur remplit toutes les conditions, Identity Manager effectue les actions spécifiées dans le champ Action lors de l'application de la stratégie. Par exemple, définissez les conditions de stratégie comme suit. intersection (who are members of <un_rôle>) and (who are members of <un_autre_rôle>)
Action lors de l'application de la stratégie	Actions qu'Identity Manager doit effectuer lorsque les conditions de stratégie s'appliquent ; par exemple : ■ Message de violation de conformité : l'utilisateur a des rôles mutuellement exclusifs ■ Supprimer le membre du <un_rôle>

La figure suivante présente la stratégie d'identité utilisée dans cet exemple.

Stratégies d'identité

Ensemble de stratégies

	Nom de la stratégie	Règle du membre de stratégie	Action lors de l'application de la stratégie
	Restrictions	Intersection (membres de (rôle d'administration "Gestionnaire d'utilisateurs") et membres de (rôle d'administration "Approbateur d'utilisateurs"))	Message de violation de la conformité : utilisateur dispose des droits mutuellement exclusifs Supprimer le membre du rôle d'administration Approbateur d'utilisateurs

Stratégies d'identité préventives

Une *stratégie d'identité préventive* est un type de stratégie d'identité qui empêche les utilisateurs de se voir attribuer des droits susceptibles d'engendrer un conflit d'intérêt ou une fraude. Ces stratégies prennent en charge les exigences de séparation des fonctions d'une société.

Les stratégies d'identité préventives, qui s'exécutent avant la soumission d'une tâche, permettent à un administrateur de rechercher les éventuelles violations de stratégie avant d'affecter des droits ou de modifier des attributs de profil. S'il existe une violation, l'administrateur peut la résoudre avant de soumettre la tâche.

Par exemple, une société peut créer une stratégie d'identité préventive qui empêche les utilisateurs disposant du rôle Gestionnaire d'utilisateurs de disposer également du rôle Approbateur d'utilisateurs. Si un administrateur utilise la tâche Modifier un utilisateur pour donner au gestionnaire d'utilisateurs le rôle d'approbateur d'utilisateurs, CA IdentityMinder affiche un message indiquant la violation. L'administrateur peut alors modifier les affectations de rôle pour résoudre la violation avant de soumettre la tâche.

Vous pouvez créer des stratégies d'identité préventives pour les changements suivants.

- **Appartenance à un rôle**

  Empêche les utilisateurs de disposer simultanément de certains rôles.

  Par exemple, les utilisateurs ne peuvent pas cumuler les rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs.

- **Administrateurs de rôles**

  Empêche les utilisateurs d'être administrateurs de certains rôles s'ils sont administrateurs d'autres rôles.

  Par exemple, les utilisateurs ne peuvent pas être simultanément administrateurs des rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs.

- **Attributs de l'utilisateur**

  Empêche les utilisateurs de posséder simultanément certains attributs de profil.

  Par exemple, les utilisateurs ne peuvent pas avoir le titre Chef comptable et être membre du département informatique.

- **Attributs de l'organisation**

  Empêche la création de profils d'utilisateur dans une certaine organisation.

  Par exemple, les administrateurs ne peuvent pas créer de profils d'employé dans l'organisation Fournisseurs.

- **Attributs de groupe**

  Empêche les utilisateurs d'être membres de certains groupes.

  Par exemple, les utilisateurs ne peuvent pas être membres des groupes Equipe de projet et Comptabilité.

Informations complémentaires :

Actions en cas de violations de stratégie d'identité préventive (page 300)

Actions en cas de violations de stratégie d'identité préventive

Lorsqu'une stratégie d'identité préventive s'applique à une modification métier, CA exécute certaines actions pour résoudre la violation.

Lorsque vous spécifiez une de ces actions dans une stratégie d'identité, vous rédigez un message qui décrit la violation. Ce message est enregistré dans la base de données d'audit. En fonction du type d'action, le message peut également s'afficher dans la console d'utilisateur et être enregistré dans la fenêtre Afficher les tâches soumises.

Pour une stratégie d'identité préventive, vous pouvez configurer les actions suivantes.

Accepter

CA IdentityMinder affiche, dans la fenêtre Afficher les tâches soumises, un message qui décrit la violation mais autorise la soumission de la tâche.

Rejeter

CA IdentityMinder affiche un message dans la console d'utilisateur et empêche la soumission de la tâche.

Avertissement

CA IdentityMinder affiche un message dans la console d'utilisateur et dans la fenêtre Afficher les tâches soumises. Cette action peut éventuellement déclencher un processus de flux de travaux qui exige l'approbation d'un utilisateur approprié avant que CA IdentityMinder exécute la tâche.

Pour déclencher un processus de flux de travaux, vous associez la stratégie d'identité préventive à un processus de flux de travaux utilisant une stratégie (page 307) dans les tâches susceptibles d'entraîner la violation.

Par exemple, si la violation se produit lorsqu'un utilisateur reçoit simultanément certains rôles, configurez le processus de flux de travaux pour toutes les tâches qui affectent ces rôles à des utilisateurs.

Remarque : Lorsque vous configurez le processus de flux de travaux utilisant une stratégie pour la tâche, la règle d'approbation doit faire référence au nom de la stratégie d'identité préventive.

Fonctionnement des stratégies d'identité préventives

L'exemple de processus suivant illustre le fonctionnement des stratégies d'identité préventives.

1. Un administrateur de stratégie d'identité crée une stratégie d'identité préventive qui empêche les utilisateurs possédant le titre de Chef comptable de faire partie du département informatique.

   Lors de la définition de cette stratégie d'identité, l'administrateur spécifie que CA IdentityMinder doit rejeter tous les changements occasionnant une violation de cette stratégie.

2. Un administrateur RH utilise la tâche Créer un utilisateur pour créer un profil d'utilisateur pour un nouveau Chef comptable. Il sélectionne bien le titre de l'utilisateur, mais choisit par erreur le département informatique.

3. Il complète tous les autres champs de la tâche Créer un utilisateur et clique sur Soumettre.

4. CA IdentityMinder détecte que la tâche comporte des changements définis dans une stratégie d'identité et vérifie s'ils entraînent des violations.

5. CA IdentityMinder détecte la violation, affiche un message à l'administrateur RH et empêche la soumission de la tâche.

   CA IdentityMinder enregistre également le message dans la base de données d'audit.

6. L'administrateur RH voit les détails de la violation dans le message et modifie le département de l'utilisateur en Finances. Ensuite, il ressoumet la tâche.

7. CA IdentityMinder évalue les changements proposés par rapport à toutes les stratégies d'identité applicables et autorise la soumission de la tâche Créer un utilisateur.

Remarques importantes concernant les stratégies d'identité préventives

Avant d'implémenter des stratégies d'identité préventives, tenez compte des informations suivantes.

- Les stratégies d'identité préventives n'empêchent que les violations qui surviendraient en raison des changements proposés dans la tâche actuelle, mais pas les violations existantes.

  Par exemple, une société crée une stratégie d'identité préventive qui empêche les utilisateurs de cumuler les rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs. Un administrateur affecte le rôle Gestionnaire de groupes à un utilisateur cumulant déjà les rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs. CA IdentityMinder autorise la réussite de l'affectation parce que ce changement n'entraîne pas directement une violation de la stratégie.

- Si plusieurs stratégies d'identité préventives s'appliquent à un ensemble de changements proposés, CA IdentityMinder applique en priorité les stratégies comportant des actions Rejeter.

- Ne spécifiez pas de groupes dynamiques dans des conditions de stratégie d'identité préventive. Les conditions de stratégie déterminent l'ensemble d'utilisateurs auquel s'applique la stratégie d'identité préventive.

  Par exemple, une société comporte un groupe dynamique qui inclut tous les utilisateurs ayant le titre Gestionnaire. Cette société crée aussi une stratégie d'identité préventive qui empêche les membres du groupe Gestionnaires de remplir le rôle Sous-traitant.

  Un administrateur change le titre d'un utilisateur ayant le rôle Sous-traitant en Gestionnaire. L'utilisateur ne deviendra toutefois membre du groupe Gestionnaires qu'*après* la réussite de la soumission de la tâche. L'utilisateur n'a donc pas le titre de Gestionnaire au moment où CA IdentityMinder évalue la stratégie, de sorte qu'aucune violation n'est détectée.

- Les filtres de propriétaire de rôle et de requête LDAP ne sont pas pris en charge dans les conditions des stratégies d'identité préventives.

Création d'une stratégie d'identité préventive

Avant de créer une stratégie d'identité préventive, vous créez un ensemble de stratégies d'identité qui, en toute logique, est destiné à les regrouper.

Remarque : Avant de commencer, reportez-vous à la rubrique Remarques importantes concernant les stratégies d'identité préventives (page 302).

Pour créer un ensemble de stratégies d'identité préventives

1. Ouvrez Stratégies, puis Créer un ensemble de stratégies d'identité dans la console d'utilisateur.

   Créez un nouvel ensemble de stratégies d'identité ou utilisez-en un existant en tant que modèle.

2. Définissez le profil de l'ensemble de stratégies d'identité (page 279)sous l'onglet Profil.

3. Créez une règle de membre de l'ensemble de stratégies (page 280) sous l'onglet Stratégies.

4. Créez une stratégie d'identité préventive comme suit.

   a. Cliquez sur Ajouter.

   b. Entrez le nom de la stratégie d'identité.

      Remarque : Les paramètres Appliquer une fois et Conformité ne s'appliquent pas aux stratégies d'identité préventives.

   c. Dans la section Condition de stratégie, identifiez les utilisateurs auxquels la stratégie s'applique.

      Remarque : Les filtres de propriétaire de rôle et de requête LDAP ne sont pas pris en charge pour les stratégies d'identité préventives.

d. Dans le champ Action lors de l'application de la stratégie, définissez les actions que CA IdentityMinder doit effectuer lorsque CA IdentityMinder détecte une violation de stratégie.

Accepter

CA IdentityMinder affiche un message dans la fenêtre Afficher les tâches soumises qui décrit la violation, mais autorise la soumission de la tâche.

Rejeter

CA IdentityMinder affiche un message dans la fenêtre Afficher les tâches soumises qui décrit la violation et interdit la soumission de la tâche.

Avertissement

CA IdentityMinder affiche un message dans la console d'utilisateur et dans la fenêtre Afficher les tâches soumises. Cette action peut éventuellement déclencher un processus de flux de travaux (page 305).

Lorsque vous sélectionnez l'une de ces actions, CA IdentityMinder affiche une zone de texte dans laquelle vous pouvez spécifier le message qui apparaît en cas de violation.

e. Spécifiez le message dans la zone de texte.

Remarque : Si vous localisez la console d'utilisateur, vous pouvez spécifier une clé de ressource au lieu du texte dans le champ du message. Reportez-vous au manuel *User Console Design Guide* pour plus d'informations sur les clés de ressource.

f. Ajoutez d'autres actions si nécessaire, puis cliquez sur OK.

5. Spécifiez les propriétaires de l'ensemble de stratégies d'identité. (page 290)

Remarque : Avant d'utiliser l'ensemble de stratégies d'identité que vous avez créé, vérifiez d'abord que vous avez activé les stratégies d'identité dans la console de gestion. Pour plus d'informations, reportez-vous au *manuel de configuration*.

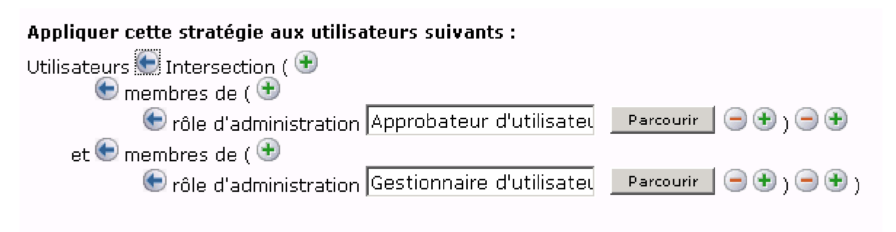
Cas d'utilisation : Prévention des conflits de rôles pour les utilisateurs

Forward, Inc. souhaite empêcher que ses employés cumulent les rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs. Les employés disposant simultanément de ces deux rôles peuvent en effet modifier des attributs d'utilisateur, comme le salaire, et les approuver de manière inappropriée.

Pour éviter cette situation, Forward, Inc. crée une stratégie d'identité préventive qui s'applique aux utilisateurs cumulant les rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs. Si un administrateur tente d'octroyer ces rôles à un utilisateur, CA IdentityMinder rejette la soumission de tâche et affiche un message expliquant la violation.

Pour résoudre ce cas d'utilisation, vous configurez une stratégie d'identité préventive comme suit.

- Créez un ensemble de stratégies d'identité pour la stratégie que vous souhaitez créer.
- Créez une stratégie d'identité préventive présentant les paramètres suivants.
  - Condition de stratégie :



  - Action lors de l'application de la stratégie :
    - Rejet avec message : l'utilisateur ne peut pas être membre des rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs

Flux de travaux et stratégies d'identité préventives

Lorsqu'une stratégie d'identité préventive est configurée pour émettre un avertissement, vous pouvez définir un processus de flux de travaux utilisant une stratégie de niveau tâche, lequel est associé à une stratégie d'identité, pour les tâches susceptibles de déclencher une violation. Par exemple, si une stratégie d'identité empêche les chefs comptables d'être membre du département informatique, vous définissez un processus de flux de travaux utilisant une stratégie de niveau tâche dans les tâches Créer un utilisateur et Modifier un utilisateur.

Toutes les tâches générées à la suite d'un flux de travaux utilisant des stratégies de niveau tâche doivent être approuvées avant que CA IdentityMinder exécute la tâche. Les approbateurs voient une tâche de liste de travail lorsqu'ils se connectent à la console d'utilisateur. Quand l'approbateur clique sur la tâche de liste de travail, une tâche d'approbation, qui inclut le message décrivant la violation, s'affiche. L'approbateur peut choisir d'approuver ou de rejeter la tâche, en fonction de la violation.

Les processus de flux de travaux utilisant des stratégies sont associés aux stratégies d'identité préventives par le nom de stratégie.

Informations complémentaires :

Flux de travaux utilisant des stratégies (page 472)

Violations des stratégies d'identité dans les tâches d'approbation

Lorsqu'une stratégie d'identité préventive est associée au processus de flux de travaux d'une tâche, CA IdentityMinder génère une liste de tâches pour les approbateurs appropriés. Ces approbateurs utilisent une tâche d'approbation pour approuver ou rejeter la modification à l'origine de la violation de stratégie.

La tâche d'approbation par défaut inclut une section qui reprend les violations de stratégie d'identité. Il pourrait s'agir de plusieurs violations si les changements proposés déclenchent plusieurs stratégies d'identité préventives.

Chaque violation peut avoir l'un des états suivants.

- **Evaluation en attente**

  CA IdentityMinder n'a pas encore commencé à évaluer les règles d'approbation pour la tâche. Il s'agit de l'état initial.

- **En attente d'approbation**

  CA IdentityMinder a trouvé une correspondance pour la stratégie d'identité définie dans les règles d'approbation et déclenché le processus de flux de travaux associé.

- **Approuvé**

  Un approbateur a approuvé les changements proposés. CA IdentityMinder apporte les modifications ayant déclenché les violations de stratégie d'identité préventives.

- **Rejeté**

  Un approbateur a rejeté le changement proposé. La tâche est rejetée.

- **Aucun flux de travaux configuré**

  Aucun processus de flux de travaux n'est configuré pour cette violation. La tâche s'exécute sans nécessiter d'approbation.

Configuration d'un flux de travaux pour des stratégies d'identité préventives

Vous configurez un flux de travaux pour des stratégies d'identité préventives dans les tâches d'administration qui incluent des changements susceptibles d'entraîner une violation de la stratégie d'identité.

Par exemple, si la stratégie d'identité préventive empêche les utilisateurs de cumuler certains rôles d'administration, configurez des tâches qui affectent des rôles d'administration pour soutenir le flux de travaux des stratégies d'identité préventives.

Remarque : Avant de configurer un flux de travaux, créez une stratégie d'identité préventive présentant les paramètres suivants.

- Nom de stratégie unique

  Le nom de la stratégie doit être unique parmi tous les ensembles de stratégies d'identité étant donné que les processus de flux de travaux sont associés aux stratégies d'identité préventives par le nom de la stratégie.

  Si plusieurs stratégies d'identité préventives portent le même nom, plusieurs processus de flux de travaux peuvent s'appliquer.

- Avertissement dans le champ Action lors de l'application de la stratégie

  Un avertissement est la seule action susceptible de déclencher un processus de flux de travaux.

Après avoir configuré la stratégie d'identité préventive, déterminez les tâches susceptibles de déclencher la violation de stratégie. Ensuite, créez une stratégie d'approbation de flux de travaux (page 308) pour ces tâches.

Création d'une stratégie d'approbation de flux de travaux pour des stratégies d'identité préventives

Vous pouvez configurer un processus de flux de travaux utilisant des stratégies de niveau tâche pour une tâche d'administration. Ce processus de flux de travaux inclut une ou plusieurs stratégies d'approbation capables d'associer une stratégie d'identité préventive à un flux de travaux. CA IdentityMinder exécute alors le flux de travaux en cas de violation de la stratégie d'identité préventive associée.

Remarque : Pour plus d'informations sur les processus de flux de travaux utilisant des stratégies de niveau tâche, reportez-vous à la rubrique Flux de travaux utilisant des stratégies (page 472).

Pour créer une stratégie d'approbation de flux de travaux pour des stratégies d'identité préventives

1. Modifiez les tâches d'administration qui autorisent les modifications susceptibles de déclencher une violation de stratégie d'identité préventive.

   Par exemple, si une violation de stratégie d'identité a lieu lorsqu'un utilisateur cumule les rôles Gestionnaire d'utilisateurs et Approbateur d'utilisateurs, modifiez les tâches d'administration qui permettent aux administrateurs d'affecter des rôles, comme Créer un utilisateur, Modifier un utilisateur et Modifier les membres/administrateurs avec rôle d'administration.

2. Cliquez sur l'icône Modifier en regard du champ Processus de flux de travaux sous l'onglet Profil de la tâche pour ajouter un processus de flux de travaux.

   CA IdentityMinder affiche la fenêtre Configuration du flux de travaux de niveau tâche.

3. Sélectionnez Utilisant des stratégies, puis cliquez sur Ajouter.

4. Dans la section Règle d'approbation, sélectionnez l'objet Violation de la stratégie d'identité.

5. Dans le champ Stratégie d'identité, sélectionnez un filtre qui détermine quelles stratégies d'identité déclenchent le flux de travaux associé à la stratégie d'approbation.

   Dans le filtre, indiquez le nom de la stratégie d'identité, *pas* celui de l'ensemble de stratégies d'identité.

6. Configurez les champs Evaluation des règles, Ordre de stratégies et Description de la stratégie comme nécessaire.

7. Sélectionnez un processus de flux de travaux, puis cliquez sur OK.

   Lorsque vous sélectionnez un processus de flux de travaux, CA IdentityMinder affiche des champs supplémentaires.

8. Spécifiez les tâches d'approbation et les approbateurs comme requis.

   CA IdentityMinder associe le processus de flux de travaux à la stratégie d'identité préventive.

Cas d'utilisation : Approbation de titres

Une des stratégies de Forward, Inc stipule que tous les gestionnaires doivent être employés à temps plein. Toutefois, Forward, Inc a récemment engagé de nombreux sous-traitants pour des projets spéciaux. Pour exécuter efficacement ces projets spéciaux, certains de ces sous-traitants se verront attribuer le titre de Gestionnaire. Forward, Inc souhaite obtenir l'approbation du directeur des Ressources humaines avant d'autoriser les administrateurs à affecter le titre de Gestionnaire à un sous-traitant.

Pour automatiser le processus d'approbation dans ces situations, Forward, Inc crée une stratégie d'identité préventive, dénommée Titres de Gestionnaire pour les sous-traitants, qui détecte lorsque le titre d'un utilisateur est Gestionnaire et lorsque l'organisation de l'utilisateur est Sous-traitant. Forward, Inc configure également un processus d'approbation utilisant une stratégie sur la tâche Modifier un utilisateur. Ce processus d'approbation est déclenché en cas de violation de la stratégie Titres de Gestionnaire pour les sous-traitants.

Lorsqu'un administrateur modifie le titre d'un sous-traitant en Gestionnaire, CA IdentityMinder affiche un message d'avertissement et envoie une tâche au directeur des Ressources humaines pour approbation. CA IdentityMinder ne modifie pas le titre du sous-traitant tant que la tâche n'a pas été approuvée.

Pour configurer ce cas d'utilisation, exécutez les actions suivantes dans CA IdentityMinder.

- Créez une stratégie d'identité préventive dénommée Titres de Gestionnaire pour les sous-traitants et présentant les paramètres suivants.
  - Condition de stratégie : Utilisateurs où (Titre = "Gestionnaire" et Organisation = "Sous-traitant")
  - Action lors de l'application de la stratégie : Avertissement avec message "Les gestionnaires doivent être des employés à temps plein."
- Modifiez la tâche Modifier un utilisateur pour inclure un processus de flux de travaux présentant les paramètres suivants.
  - Processus de flux de travaux : Utilisant des stratégies
  - Objet Règle d'approbation : Violation d'une stratégie d'identité
  - Stratégie d'identité : où (Nom = "Titres de Gestionnaire pour les sous-traitants")
  - Processus de flux de travaux : SingleStepApproval

Combinaison de stratégies d'identité et de stratégies d'identité préventives

Vous pouvez combiner des stratégies d'identité et des stratégies d'identité préventives pour satisfaire aux besoins de séparation des fonctions. Dans ce cas, les stratégies d'identité corrigent les violations de séparation des fonctions existantes et les stratégies d'identité préventives en empêchent de nouvelles.

Pour prendre en charge ce cas d'utilisation, vous configurez un ensemble de stratégies d'identité avec les deux types d'actions suivants.

- Actions se produisant pendant la synchronisation des utilisateurs

  Ces actions donnent lieu à des changements des attributs d'utilisateur, des membres de groupe et de rôle, des administrateurs ou des propriétaires. Par exemple, une action de ce type peut supprimer un utilisateur d'un rôle en cas de détection d'une violation.

  Ces actions diffèrent des préventives dans le sens où elles ne sont pas appliquées lors de la soumission d'une tâche, mais uniquement pendant la synchronisation des utilisateurs (page 291).

- Actions préventives

  Ces actions déterminent le comportement de CA IdentityMinder en cas de violation d'une stratégie d'identité préventive *avant* la soumission d'une tâche. CA IdentityMinder peut autoriser la soumission de la tâche, l'empêcher ou émettre un avertissement et déclencher un processus de flux de travaux.

  Dans chacun de ces cas, la violation est enregistrée dans la base de données d'audit.

Imaginez une société qui souhaite empêcher que des utilisateurs endossent simultanément les rôles Administrateur RH et Approbateur de salaire. Cette société crée une stratégie d'identité avec deux actions lors de l'application de la stratégie.

- Supprimer l'utilisateur du rôle Approbateur de salaire

  Cette action se produit lorsque CA IdentityMinder synchronise les utilisateurs avec des stratégies d'identité.

  Dans ce cas, la société a configuré la synchronisation des utilisateurs pour la tâche Modifier un utilisateur. Lorsqu'un administrateur modifie un utilisateur, CA IdentityMinder évalue toutes les stratégies d'identité pertinentes et applique les actions. Dans cet exemple, CA IdentityMinder supprime du rôle Approbateur de salaire les utilisateurs cumulant ce rôle avec celui d'Administrateur RH.

- Rejeter la tâche

  Cette action préventive empêche les administrateurs d'affecter ces deux rôles à une même personne en interdisant à l'administrateur de soumettre la tâche.

Remarque : Lorsque vous configurez une stratégie d'identité avec ces deux types d'action, vérifiez que les actions ne soient pas en conflit. Par exemple, vous pouvez configurer une stratégie d'identité qui empêche les utilisateurs de cumuler les rôles Gestionnaire et Sous-traitant. Dans la stratégie, vous spécifiez deux actions.

- Un avertissement qui déclenche un processus de flux de travaux, lequel nécessite une approbation avant l'affectation des rôles.
- Une action qui supprime un utilisateur du rôle Gestionnaire.

Un approbateur approuve l'affectation des rôles Gestionnaire et Sous-traitant, mais la seconde action supprime l'utilisateur du rôle Gestionnaire lors de la synchronisation des utilisateurs.

Chapitre 14: IM_12.6.1 : Application mobile CA IdentityMinder

L'application mobile CA IdentityMinder permet d'exploiter l'infrastructure CA IdentityMinder existante pour permettre aux utilisateurs d'effectuer les tâches suivantes sur une unité mobile, telle qu'un iPhone ou un iPad :

- Réinitialisation d'un mot de passe oublié

  Remarque : Lorsque vous permettez aux utilisateurs mobiles de réinitialiser un mot de passe oublié à partir de leur unité, CA IdentityMinder utilise la sécurité de l'unité au lieu de questions de sécurité. Envisagez d'exiger une sécurité de l'unité supplémentaire, tel qu'un code secret avant d'activer la fonctionnalité de réinitialisation de mot de passe.

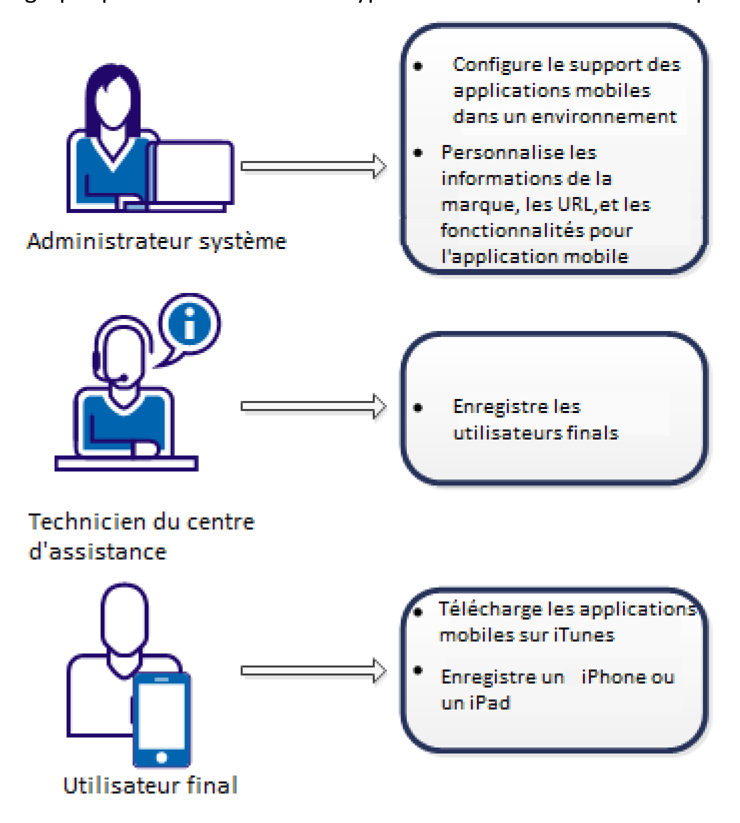
- Modification d'un mot de passe
- Réponse aux demandes d'approbation
- Affichage des détails du gestionnaire

  Cette fonctionnalité permet aux utilisateurs qui approuvent des demandes de flux de travaux d'afficher des informations sur le gestionnaire d'un utilisateur.

Ce chapitre traite des sujets suivants :

Fonctionnement du processus d'implémentation

Trois types d'utilisateurs sont concernés par la configuration d'applications mobiles. Le graphique suivant illustre ces types d'utilisateur et les tâches qu'ils effectuent.



Pour permettre à un utilisateur final d'utiliser l'application mobile avec CA IdentityMinder, les actions suivantes doivent être réalisées :

1. Un administrateur système configure la prise en charge de l'application mobile dans un environnement.

   La configuration implique les actions suivantes :

   - Configuration des attributs de code d'activation
   - Ajout de tâches, de stratégies Policy Xpress et d'un modèle de courriel pour l'enregistrement d'utilisateurs de téléphone portable
   - Création d'une définition de services Web
   - Modification du courriel d'enregistrement

   L'administrateur système configure également la personnalisation, les URL et la fonctionnalité à laquelle les utilisateurs de téléphone portable peuvent accéder.

2. Un administrateur, par exemple un technicien du centre d'assistance, enregistre les utilisateurs finals concernés dans la console d'utilisateur.

   Le processus d'enregistrement déclenche un code d'activation pour chaque utilisateur final et leur envoie automatiquement un courriel contenant le code et les instructions d'enregistrement.

3. L'utilisateur final télécharge l'application mobile à partir d'iTunes Store et enregistre une unité, tellle qu'un iPhone ou un iPad, à l'aide des instructions et du code reçus dans le courriel.

   L'utilisateur final peut alors utiliser l'application mobile pour accéder à la fonctionnalité CA IdentityMinder.

Configuration de CA IdentityMinder pour la prise en charge d'applications mobiles

L'application mobile communique avec CA IdentityMinder pour gérer des mots de passe et des approbations. Pour activer cette communication, un administrateur système effectue les étapes suivantes :

1. Configuration des attributs de code d'activation (page 316)
2. Ajout de nouvelles tâches à un environnement par l'importation de fichiers de définitions de rôles (page 318)
3. Création d'un service Web REST (page 319)
4. Modification du courriel d'enregistrement (page 320)

Configuration des attributs de code d'activation

Pour activer l'enregistrement d'utilisateurs et l'accès à travers l'application mobile, le référentiel d'utilisateurs CA IdentityMinder doit inclure les attributs reconnus suivants :

- %ACTCODE%
- %ACTCODEVAL%

Remarque : Mappez ces attributs reconnus vers des attributs du référentiel d'utilisateurs disponibles dans le fichier de configuration d'annuaire (directory.xml). Si aucun attribut n'est disponible, développez le schéma du référentiel d'utilisateurs. Pour obtenir un exemple de développement d'un référentiel d'utilisateurs CA Directory, consultez

Procédez comme suit:

1. Connectez-vous à la console de gestion.
2. Sélectionnez Répertoires, puis cliquez sur le répertoire contenant des utilisateurs de téléphone portable.
3. Exportez le répertoire.
4. Ajoutez ou modifiez des descriptions d'attributs pour inclure l'attribut reconnu %ACTCODE%.

   Vous pouvez mapper un attribut disponible vers l'attribut connu %ACTCODE%.

   ```
   <ImsManagedObjectAttr
   physicalname="attr1"
   displayname="ActivationCode"
   description="Activiation Code"
   valuetype="String"
   required="false"
   multivalued="false"
   wellknown="%ACTCODE%"
   maxlength="0" />
   ```

5. Pour définir l'attribut reconnu %ACTCODEVAL%, répétez l'étape 4.
6. Enregistrez le fichier directory.xml.
7. Pour charger le fichier directory.xml enregistré, cliquez sur Mettre à jour dans la page Directory Properties (Propriétés de répertoire) de la console de gestion.

Exemple : Développement du schéma CA Directory

L'exemple suivant décrit les étapes de développement d'instance CA Directory personnalisée pour inclure des attributs de code d'activation et de valeur de code d'activation.

Remarque : Envisagez le développement d'un schéma personnalisé, non du schéma par défaut. Le schéma par défaut est remplacé lors des mises à niveau.

Si vous utilisez un type de référentiel d'utilisateurs différent, utilisez la documentation fournie avec ce référentiel pour développer le schéma.

Procédez comme suit:

1. Modifiez l'objectclass de l'appliance de stockage de données (DSA).

   Par exemple, modifiez %DIR_HOME%\dxserver\config\schema*custom_schema*.dxc comme suit :

   ```
   schema set attribute (1.3.6.1.4.1.2552.2.2.3.228) = {
      name = acctCode
      ldap-names = actCode
      syntax = caseIgnoreString
      single-valued
   };
   schema set attribute {1.3.6.1.4.1.2552.2.2.3.229) = {
      name = actCodeVal
      ldap-names = acctCodeVal
      syntax = caseIgnoreString
      single-valued
   };
   ```

   Remarque : Dans l'exemple ci-dessus, .228 et .229 sont des exemples de nombres. Consultez le schéma personnalisé pour obtenir les nombres disponibles.

2. Ajoutez les nouveaux attributs au schéma objectclass comme suit :

   ```
   ###############################################################

   ## Custom Object Class (optional)

   ##############################################################

   schema set object-class (1.3.6.1.4.1.2552.2.2.3.0) = {
      name = IDMPerson
      ldap-names = IDMPerson
      inetOrgPerson sous-classe-de
      may-contain
         IDMAdminRoles,
         IDMDisabled,
         IDMForgottenQuestions,
         IDMPasswordData,
         IDMIdentityPolicy,
         IDMCertStatus,
   ```

```
        IDMLastCertified,
        managerID,
        departmentID,
        jobFamily,
        jobCode,
        band,
        QuestionsAnswered,
        IDMDevices,
        IDMApprovalDelegation,
        country,
        acctCode,
        acctCodeVal
    };
```

3. Redémarrez l'appliance de stockage de données pour charger le nouveau schéma en saisissant les commandes suivantes dans la ligne de commande :

   dxserver stop *env_name*

   dxserver start *env_name*

Importation de tâches d'administration

Avant que les utilisateurs de téléphone portable puissent se connecter à CA IdentityMinder, les administrateurs les enregistrent dans la console d'utilisateur. Le processus d'enregistrement génère un code d'activation et envoie un courriel à l'utilisateur de téléphone portable.

Pour prendre en charge ces activités, importez un fichier de définition de rôle qui ajoute la fonctionnalité suivante à un environnement :

- Enregistrement d'utilisateur d'application mobile et suppression d'utilisateur de tâches d'applications mobiles
- Stratégie Policy Xpress générant et validant les codes d'activation d'applications mobiles. Une stratégie Policy Xpress annule également l'enregistrement du client de téléphone portable à partir d'un compte d'utilisateur.
- Modèle de courriel pour l'envoi du courriel aux utilisateurs de téléphone portable

Procédez comme suit:

1. Connectez-vous à la console de gestion.
2. Sélectionnez Environnements, puis cliquez sur l'environnement qui prend en charge l'application mobile.
3. Dans la fenêtre suivante, sélectionnez Role and Task Settings (Paramètres des rôles et des tâches), puis cliquez sur Importer.

4. Sélectionnez MobileApp-RoleDefinitions, puis cliquez sur Terminer.
5. Redémarrez l'environnement.
6. Ajoutez les tâches suivantes au rôle de responsable du système :
   - Enregistrement d'utilisateur de l'application mobile
   - Suppression d'utilisateur de l'application mobile

   Les nouvelles tâches se trouvent dans la catégorie Utilisateur.

Création d'un service Web REST

L'application mobile utilise des services Web REST pour communiquer avec CA IdentityMinder. Pour prendre en charge l'application mobile, un administrateur système crée une définition de service Web dans la console d'utilisateur.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur en tant qu'utilisateur disposant de droits d'administrateur système.
2. Créez une définition de service Web comme suit :
   a. Ouvrez Système, Services Web, Create Web Services (Créer des services Web).
   b. Dans l'onglet Profil, renseignez les champs suivants :
      - Nom : RestMobile
      - Identificateur : *identificateur unique* La valeur par défaut est RestMobile.

        La valeur du champ Identificateur doit correspondre à la valeur de **restid** dans la configuration d'application mobile.

        Pour plus de sécurité, pensez à modifier la valeur de l'identificateur et de restid.
      - Enable Attribute (Activer l'attribut) : sélectionnez cette case à cocher.

      Ne modifiez pas les paramètres de l'onglet Security.
   c. Dans l'onglet Type d'objet, sélectionnez Utilisateur comme type d'objet.
   d. Dans l'onglet Auto-administration, procédez comme suit :
      - Créez un rôle de membre et spécifiez Tout.
      - Activez la réinitialisation de mot de passe pour prendre en charge la fonctionnalité Modifier le mot de passe dans l'application mobile.
   e. Dans l'onglet Membre, créez une règle de membre avec les critères suivants :
      - Code d'activation : enregistré, ou
      - Code d'activation >0
   f. Enregistrez le service Web.

Modification du courriel d'enregistrement

Modifiez le courriel d'enregistrement par défaut pour inclure l'URL du serveur de configuration d'application mobile (MACS) (page 321).

Procédez comme suit:

1. Dans la console d'utilisateur, sélectionnez Système, Courriel, Modifier le courriel.
2. Rechercher et sélectionnez l'utilisateur enregistré pour le courriel d'application mobile.
3. Dans l'onglet Contenu, cliquez sur Toggle HTML Source (Basculer vers la source HTML).
4. Spécifiez l'URL des serveurs MAC dans l'entrée href pour mobileregservidm comme suit :

    <a href="mobileregservidm://{'Attribute:%ACTCODE%'}&https://*macserver*/macs/rest/caidm/*default*">

    macserver

    Spécifiez le nom ou l'adresse IP des serveurs MAC.

    default

    Spécifiez le nom du fichier JSON de configuration dans les serveurs MAC. Le nom par défaut est defaultRegistration.json.

5. Cliquez sur Soumettre.

Serveur de configuration d'application mobile (MACS)

MACS permet aux administrateurs système de configurer l'application mobile CA IdentityMinder.

MACS lit les informations de configuration à partir d'un fichier JSON et configure l'application mobile lorsque l'utilisateur de téléphone portable se connecte avec un iPhone ou un iPad.

Remarque : La version actuelle inclut un exemple d'interface utilisateur MACS qui permet aux administrateurs de saisir les informations de configuration dans les champs au lieu de modifier directement un fichier texte. L'interface utilisateur génère le contenu JSON final à l'issue de la configuration. Vous pouvez ensuite copier le contenu JSON généré dans un fichier de configuration dans le serveur où MACS est installé. L'interface utilisateur MACS est actuellement disponible sous forme d'aperçu technique.

Pour plus d'informations sur l'utilisation de l'interface utilisateur MACS, recherchez la section *Scenario: Utilisation de l'interface utilisateur de serveur de configuration* d'application mobile sur le site du support.

Les administrateurs peuvent configurer les propriétés de configuration suivantes pour l'application mobile :

- Personnalisation

  Spécifiez le logo de la société dans l'application mobile.

- Fonctionnalité

  Activez la fonctionnalité suivante :

  - Prise en charge de mot de passe oublié
  - Prise en charge de la réinitialisation de mot de passe
  - File d'attente d'approbation de flux de travaux
  - Affichage du lien du gestionnaire

- Options de prise en charge et d'aide

  Spécifiez les informations de contact pour le support, ajoutez un message d'aide et décrivez les restrictions de stratégie de mot de passe.

- Mappage d'attributs

  Dans le référentiel d'utilisateurs, mappez des attributs vers des attributs inclus dans l'application mobile.

Les administrateurs configurent également les services Web REST qui permettent la communication entre un environnement CA IdentityMinder et l'application mobile.

Lorsqu'un utilisateur de téléphone portable se connecte, l'application mobile contacte MACS à l'aide des services Web REST. MACS configure alors l'application mobile avec les paramètres appropriés définis dans la configuration.

Installation du serveur de configuration d'application mobile

Le serveur de configuration d'application mobile (MACS) permet aux administrateurs système de configurer des paramètres pour le client d'application mobile. Le client reçoit ces paramètres lors de l'exécution, lorsqu'un utilisateur de téléphone mobile se connecte au client sur son iPhone ou son iPad.

Procédez comme suit:

1. Sur un système contenant les outils d'administration CA IdentityMinder, accédez au répertoire MobileApplication.

   Par exemple, sur un système Windows, le répertoire MobileApplication est installé à l'emplacement suivant :

   C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\

2. Recherchez le fichier macs.war.

3. Déployez MACS sur un serveur d'applications pris en charge.

   Ne déployez pas MACS sur le même serveur d'applications que CA IdentityMinder.

   Par exemple, sur un serveur d'applications JBoss, décompressez l'archive macs.war et déployez-la comme système de fichiers dans le répertoire de déploiement :

   jboss_home\jboss-5.1.0.GA\server\default\deploy

   Remarque : Pour obtenir des instructions de déploiement de macs.war sur d'autres serveurs d'applications, consultez la documentation de la version de serveur d'applications appropriée.

Configuration d'une application mobile

Pour configurer une application mobile, un administrateur système crée un fichier JSON.

Les administrateurs système peuvent créer plusieurs fichiers pour prendre en charge différentes configurations. Par exemple, un administrateur système peut créer une configuration pour des gestionnaires qui peuvent approuver des tâches à partir de leur unité et une autre configuration pour d'autres employés qui peuvent uniquement réinitialiser des mots de passe.

Procédez comme suit:

1. Accédez à l'emplacement dans lequel vous avez déployé le fichier macs.war.
2. Décompressez l'archive macs.war et accédez au répertoire de configuration.
3. Effectuez une copie de defaultRegistration.json comme sauvegarde.
4. Ouvrez defaultRegistration.json dans un éditeur de texte.
5. Spécifiez des paramètres de configuration (page 323) et enregistrez le fichier.

Paramètre du fichier de configuration JSON

Le fichier de configuration JSON inclut les paramètres suivants :

Informations de configuration

Spécifiez des informations sur le fichier de configuration.

configName

Spécifiez le nom du fichier de configuration.

Les fichiers de configuration se trouvent dans le répertoire macs.war\conf.

confVer

Pour suivre les versions lors des modifications du fichier JSON, incrémentez cette valeur.

Remarque : N'incrémentez pas le numéro de version lors de la première modification du fichier. L'application mobile utilise le numéro de version pour déterminer le moment approprié pour télécharger une nouvelle version de la configuration.

Informations d'environnement

priAlias

Spécifiez l'alias privé pour l'environnement.

L'URL pour des tâches protégées, telles que des tâches d'approbation, inclut l'alias privé.

pubAlias

Spécifiez l'alias public pour l'environnement.

L'URL pour des tâches protégées, telles que la réinitialisation de mot de passe, inclut l'alias public.

Informations de service Web REST

Les informations sur ces entrées composent l'adresse de l'API REST de CA IdentityMinder, comme suit :

restProtocol://restServer:restPort/

restServer

Spécifiez le nom d'hôte du serveur sur lequel CA IdentityMinder est installé.

restProtocol

Spécifiez le protocole (http, https) à utiliser pour la communication entre CA IdentityMinder et l'application mobile.

restPort

Spécifiez le port de communication. Le port par défaut est 443.

restid

Spécifiez un identificateur unique pour la configuration du service Web REST.

Remarque : La valeur de restid doit correspondre à la valeur du champ Identificateur dans la définition du service Web REST.

serviceAcct

Spécifiez le nom du compte que MACS utilise pour tester les URL et réinitialiser des mots de passe.

Spécifiez un compte pouvant utiliser des services Web REST, tel que le responsable du système.

Remarque : Spécifiez des valeurs pour serviceAcct et servicePwd uniquement lorsque l'application mobile prend en charge la fonctionnalité de réinitialisation de mot de passe.

servicePwd

Spécifiez le mot de passe du compte du service.

restWait

Spécifiez la durée en secondes d'attente après l'initialisation de la modification d'un mot de passeà partir de l'application mobile. La valeur par défaut est 10 secondes.

Personnalisation

Spécifiez un logo de société ou une autre image pour l'application mobile.

brandImage

Spécifiez l'URL complète vers un fichier PNG.

Remarque : Pour simplifier l'administration, pensez à ajouter l'image au répertoire macs.war\conf.

Appliquez l'arrière-plan de l'image transparent. L'image apparaît sur un arrière-plan noir.

Paramètres de prise en charge et d'aide

Spécifiez les informations que les utilisateurs de téléphone mobile peuvent consulter dans l'onglet Support de l'application mobile.

supportEmail

Spécifiez une adresse électronique pour le service de support clientèle dans votre organisation.

supportPhone

Spécifiez le numéro de téléphone du service de support clientèle dans votre organisation.

helpMsg

Spécifiez des instructions pour les utilisateurs de téléphone portable rencontrant un problème ou ayant besoin de certaines informations supplémentaires.

Par exemple, spécifiez un message similaire au texte suivant :

Cette application est fournie par *nom de votre société* aux fins d'utilisation professionnelle uniquement. \n\n En cas de problèmes, contactez le centre d'assistance au *numéro_téléphone_support* ou à l'adresse *courriel_support.*

pwdPolicy

Fournissez des détails sur les stratégies de mots de passe qui s'appliquent. Ces informations aident les utilisateurs de téléphone portable qui veulent réinitialiser leur mot de passe à l'aide de l'application mobile.

Fonctionnalité

Vous pouvez configurer la disponibilité des fonctionnalités dans l'application mobile.

services

Répertoriez les fonctionnalités à activer pour l'application mobile. Spécifiez l'une ou plusieurs des options suivantes :

- wfApproval
- pwdReset

  Remarque : Lorsque vous permettez aux utilisateurs mobiles de réinitialiser un mot de passe oublié à partir de leur unité, CA IdentityMinder utilise la sécurité de l'unité au lieu de questions de sécurité. Envisagez d'exiger une sécurité de l'unité supplémentaire, tel qu'un code secret avant d'activer la fonctionnalité de réinitialisation de mot de passe.

- pwdChange
- hierarchyLink

  L'option hierarchyLink permet aux utilisateurs de téléphone portable d'afficher des informations sur le gestionnaire d'un utilisateur. Cette fonctionnalité peut aider des utilisateurs de téléphone portable qui approuvent des éléments de flux de travaux.

Mappage d'attributs

Spécifiez des attributs de profil d'utilisateur clés qui sont utilisés dans l'application mobile.

directory

Mappez des attributs dans l'application mobile vers des attributs figurant dans le référentiel d'utilisateurs CA IdentityMinder. Vous pouvez mapper les attributs d'application mobile suivants vers des attributs physiques ou reconnus :

- Prénom
- Nom
- titre
- Service
- Bureau
- Téléphone
- Courriel
- ID du responsable

Dépannage de l'application mobile

Si un utilisateur rencontre un problème avec l'application mobile, les ingénieurs du support peuvent demander un fichier journal aux fins de dépannage.

L'utilisateur de téléphone portable active le débogage via son iPhone ou iPad. Une fois le débogage activé, l'utilisateur de téléphone portable peut utiliser l'application mobile pour envoyer le fichier journal à une adresse électronique du support.

Pour permettre à l'application mobile de générer un fichier journal, l'utilisateur de téléphone portable doit suivre la procédure suivante.

1. Dans le téléphone ou l'iPad, accédez à Paramètres, CA IdentityMinder, Déboguer.
2. Cliquez sur Activation.
3. Redémarrez l'application et réalisez les actions que vous voulez afficher dans le journal.
4. Dans l'onglet Aide de l'application mobile CA IdentityMinder, cliquez sur Email Log (Envoyer le journal par courriel).

   L'application mobile crée un courriel avec le fichier journal joint. Le courriel est envoyé à l'adresse électronique configurée pour le support dans la configuration du serveur MACS.

Chapitre 15: Policy Xpress

Ce chapitre traite des sujets suivants :

Présentation de Policy Xpress

Policy Xpress vous permet de créer une logique métier complexe (stratégies) dans CA IdentityMinder sans développer de code personnalisé. Toutefois, les concepts impliqués lors de la création des stratégies de Policy Xpress sont complexes et doivent être soigneusement préparés et planifiés. Un administrateur utilisant des fenêtres de portail CA IdentityMinder peut configurer une stratégie dans Policy Xpress pour implémenter tout type de logique métier requise, y compris les plus exigeantes. Face aux fluctuations des processus métier, un administrateur peut modifier les stratégies à l'adie des fenêtres de configuration dans CA IdentityMinder sans requérir qu'un développeur modifie le code, et plus important encore, si les procédures de gestion sont correctement modifiées, aucun redémarrage des services CA IdentityMinder n'est requis.

Remarque : Pour plus d'informations détaillées concernant Policy Xpress, consultez la Policy Xpress Wiki https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/wiki/-/wiki/Main/Policy+Xpress?p_r_p_564233524_categoryId=0&#p_36.

Procédure de création d'une stratégie

Pour créer une stratégie à l'aide de Policy Xpress, définissez les éléments de base d'une stratégie suivants.

Profil

Définit le type de stratégie et sa priorité et permet de regrouper des stratégies similaires pour une gestion plus aisée.

Evénements

Définissent le moment d'exécution d'une stratégie.

Remarque : Veillez à définir correctement le paramètre Evénements. La logique métier doit être exécutée à des moments spécifiques pour empêcher l'endommagement de données et accroître les performances. Par exemple, un utilisateur doit être défini comme Activé lorsqu'il est créé. L'exécution de cette logique à n'importe quel moment peut réactiver des comptes utilisateur qui doivent être désactivés. Un autre exemple est l'octroi à l'utilisateur d'un rôle de provisionnement qui donne accès à un système spécifique. Ce rôle ne devrait être affecté à l'utilisateur qu'après affectation et approbation d'un autre rôle. Policy Xpress permet l'activation de sa logique métier lors du traitement du gestionnaire de tâches métier et d'événements, comme des adaptateurs personnalisés. Par conséquent, contrairement aux stratégies d'identité, la logique peut être déclenchée à tout moment, et pas seulement au début d'une tâche.

Données (éléments de données)

Spécifient les données utilisées par la stratégie. Tout type de logique métier doit utiliser des données. Ces données permettent de prendre des décisions ou de générer des données encore plus complexes. Policy Xpress fournit de nombreux composants spécifiques pour la collecte de données. Ces composants sont appelés *éléments de données*. La valeur d'attribut d'un utilisateur est un exemple d'élément de données. Par exemple, Policy Xpress peut recueillir le prénom de l'utilisateur et le stocker comme un élément de données pour l'utiliser ultérieurement.

Règles de saisie

Définissent les conditions à remplir avant l'exécution. La définition de règles de saisie vous permet de spécifier le moment où Policy Xpress évalue les stratégies, ce qui peut simplifier les stratégies et améliorer les performances. Exemple de règle de saisie : l'exécution d'une stratégie "Définition de nom complet" *uniquement* en cas de modification du prénom ou du nom.

Règles d'action

Définissent l'action entreprise en fonction des informations collectées. Par exemple, en fonction du nom du service d'un utilisateur, Policy Xpress peut affecter à un utilisateur différents rôles ou spécifier des valeurs de compte.

Actions

Spécifient l'action à effectuer. A la fin du processus, Policy Xpress effectue les actions nécessaires pour la logique métier. Policy Xpress fonctionne avec une règle d'action associée à plusieurs actions, de sorte que lorsque la règle est respectée, ces dernières sont exécutées. Les actions peuvent notamment comprendre l'affectation de valeurs d'attribut à un utilisateur ou un compte, l'exécution d'une ligne de commande ou d'une commande SQL, ou encore la génération d'un nouvel événement.

Profil

L'onglet Profil d'une stratégie Policy Xpress contient des champs qui gèrent les stratégies et ajustent leurs fonctions.

Remarque : Une stratégie s'applique uniquement à l'environnement dans lequel elle est créée. Par exemple, si vous créez une stratégie lorsque vous êtes connecté à l'environnement neteauto, la stratégie s'exécute uniquement dans cet environnement.

Lorsque vous créez une stratégie, spécifiez les informations de profil suivantes :

Nom de la stratégie

Définit un nom unique pour la stratégie.

Type de stratégie

Définit les écouteurs (page 333) qui déclenchent la stratégie. Chaque type de stratégie présente une configuration spécifique.

Remarque : Vous ne pouvez plus modifier ce champ une fois la stratégie enregistrée.

Catégorie

Définit un groupe de stratégies associées. Ce champ vous permet de regrouper des stratégies pour une gestion plus aisée.

Description

Spécifie une description de la stratégie.

Priorité

Si plusieurs stratégies sont exécutées dans le cadre d'un seul événement, ce champ spécifie le moment d'exécution de la stratégie. Les stratégies sont exécutées en fonction de leur ordre de priorité. Plus le chiffre est petit, plus la priorité est importante (la priorité 1 est exécutée en premier lieu, puis la 10, puis la 50, etc.).
La définition de priorités est utile pour les stratégies qui dépendent d'une autre ou pour la division d'une stratégie complexe en deux stratégies simples qui sont exécutées l'une après l'autre.
Imaginons, par exemple, que trois stratégies sont exécutées si une valeur spécifique est présente dans la base de données. Pour éviter que chaque stratégie ne vérifie la valeur dans la base de données, créez une stratégie qui s'exécutera avant les trois autres et qui vérifiera la valeur en question. Si la nouvelle stratégie détecte la valeur requise, Policy Xpress peut définir une variable. Les trois autres stratégies ne s'exécutent que si cette variable est définie, ce qui empêche l'accès redondant à la base de données.

Activé

Spécifie si la stratégie est active dans CA IdentityMinder. Vous pouvez désactiver cette case si vous voulez désactiver une stratégie sans la supprimer.

Exécuter une fois

Spécifie que la stratégie n'est exécutée qu'une seule fois. Il est possible que certaines stratégies doivent être exécutées à chaque fois qu'elles rencontrent des critères spécifiques, alors que d'autres peuvent ne nécessiter qu'une seule exécution. Cette valeur détermine si des règles d'action exécutées auparavant doivent l'être à nouveau.

Par exemple, l'ajout d'un rôle SAP à un utilisateur en fonction du service est une action qui doit être exécutée uniquement la première fois que l'utilisateur correspond au service. Au contraire, une stratégie qui définit le niveau de salaire de l'utilisateur en fonction de son titre *ne sera pas* définie de manière à être exécutée une seule fois, et ce afin de s'assurer qu'aucune modification non autorisée n'est apportée.

Remarque : L'option Exécuter une fois s'applique à un objet, pas à l'ensemble des objets.

Ecouteurs

Les stratégies Policy Xpress sont déclenchées par des situations qui se produisent dans le système. Pour implémenter cette fonctionnalité, les écouteurs intégrés au système signalent tout événement à Policy Xpress et lui fournissent des détails y afférents.

Les écouteurs disponibles sont les suivants :

Evénement

Détecte tous les événements du système et tous les états associés aux événements (Avant, Approuvé, Rejeté, etc.). Cet écouteur signale également le nom des événements à Policy Xpress. Les états disponibles pour l'écouteur Evénement sont les suivants :

- Avant
- Rejeté
- Approuvé
- Après
- Echec

Interface utilisateur

Détecte les différentes tâches exécutées dans le système durant l'état synchronisé, c'est-à-dire lorsque l'interface utilisateur pour cette tâche est encore ouverte. Les états disponibles pour l'écouteur Interface utilisateur sont les suivants :

- Démarrer : lorsque la tâche débute.
- Définir le sujet : lorsque l'objet principal est trouvé.
- Valider lors de la modification (page 334) : lorsqu'un attribut dont l'option Valider lors de la modification est activée, est modifié.
- Valider lors de la soumission : lorsque vous cliquez sur le bouton Soumettre.
- Soumission : lorsque la tâche est soumise.

Flux de travaux

Détecte les processus de flux de travaux qui ont trouvé des approbateurs. Cet écouteur est utile pour appliquer une logique basée sur les approbateurs, telle que l'envoi d'un courriel à l'approbateur.

Tâche soumise

Détecte les tâches soumises inactives en arrière-plan. Cet écouteur ressemble à l'écouteur Evénement, mais il considère une tâche dans son ensemble et pas les événements d'une tâche. Les états disponibles pour l'écouteur Tâche soumise sont les suivants :

- Tâche lancée
- Tâche terminée
- Echec de la tâche

Synchronisation inversée

Détecte dans le système des notifications relatives à la fonctionnalité d'exploration de CA IdentityMinder.

Validation de l'attribut à l'écran

Outre les déclencheurs définis (types de stratégie), Policy Xpress peut également écouter la validation d'attributs. Cela vous permet de créer des stratégies qui peuvent être exécutées lorsqu'un attribut à l'écran marqué comme "Valider lors de la modification" est mis à jour.

Cette fonctionnalité peut être utilisée pour créer des listes déroulantes dépendantes. Par exemple, si deux listes déroulantes sont affichées à l'écran, Policy Xpress s'exécute lorsque la sélection est effectuée dans la première liste déroulante, puis il définit les valeurs de la deuxième liste déroulante en fonction de l'option sélectionnée dans la première. Il est ainsi possible d'effectuer un nombre illimité d'actualisations de listes déroulantes et d'écrans. Cette méthode diffère de la fonction Données de boîtes de sélection car elle permet de proposer les options de listes déroulantes selon n'importe quelle logique, plutôt que par le biais de l'importation d'un fichier XML d'options statiques.

Une autre utilisation consiste à renseigner d'autres attributs sur la base de la valeur d'un attribut spécifique. Par exemple, lorsqu'un administrateur sélectionne un service, Policy Xpress peut automatiquement renseigner d'autres attributs, tels que le responsable et le numéro du service, ou encore le code du service pour les ressources humaines. Cette fonctionnalité supprime le besoin d'écrire le code personnalisé du gestionnaire d'attributs logiques.

Pour configurer la validation à l'aide d'une stratégie Policy Xpress

1. Dans la console d'utilisateur, modifiez la fenêtre de profil d'une tâche et sélectionnez le champ à écouter.
2. Allez dans les propriétés du champ et sélectionnez Oui dans la liste déroulante Valider lors de la modification.

3. Dans Policy Xpress, créez une stratégie de type "Interface utilisateur (page 333)" .
4. Dans l'onglet Evénements d'exécution, sélectionnez l'état "Valider lors de la modification" et la tâche que vous avez modifiée à l'étape 1.

Cas d'utilisation : recherche de noms choquants

Lorsqu'un utilisateur est créé, il se peut que vous souhaitiez vérifier si le nom d'utilisateur est choquant. Le processus suivant explique comment rechercher des noms choquants en utilisant une stratégie Policy Xpress.

1. Assurez-vous que les champs adéquats de l'écran Profil de la tâche Créer un utilisateur ont l'option Valider lors de la modification définie sur Oui.
2. Dans Policy Xpress, créez une stratégie de type "Interface utilisateur" .
3. Dans l'onglet Evénements d'exécution, sélectionnez l'état "Valider lors de la modification" et la tâche Créer un utilisateur.
4. Créez les éléments de données suivants pour vérifier le prénom :
   - Obtenir l'attribut du prénom (Attributs, Attribut de l'utilisateur, Obtenir)
   - Analyser toutes les minuscules du prénom (Général, Analyseur de chaînes, En minuscule)
   - Vérifier le prénom par rapport à des mots choquants figurant dans une table de base de données (Sources de données, Données de la requête SQL).
5. Créez des éléments de données similaires comme indiqué à l'étape 4 afin de vérifier le nom.
6. Créez une règle d'action comme suit :
   - Condition : le prénom est différent de "" (cela se produit si la requête renvoie un message selon lequel le nom est choquant).
   - Action : un message s'affiche (Messages, Message à l'écran), indiquant le nom choquant.

   Cette règle oblige l'utilisateur à modifier le nom avant de soumettre de nouveau la tâche Créer un utilisateur.
7. Créez une règle d'action similaire comme indiqué à l'étape 6 pour le nom.

Evénements

En fonction du type de stratégie sélectionné dans l'onglet Profil, vous pouvez configurer des moments d'activation afin de déterminer quand la stratégie est évaluée. Par exemple, une stratégie du type Evénement peut être définie pour évaluation avant un événement CreateUserEvent. Une stratégie de type Tâche peut être définie pour évaluation au moment de la définition du sujet pour l'événement DisableUserEvent.

Pour configurer un moment d'activation, sélectionnez les champs suivants :

Etat

Spécifie la durée ou l'action liée à l'événement qui active la stratégie. Par exemple, une stratégie peut être définie de manière à être exécutée "avant" qu'un événement ne se produise.

Nom de l'événement

Spécifie l'événement qui active la stratégie, comme un événement CreateUserEvent.

Une stratégie peut avoir plusieurs moments d'activation. A chaque fois qu'un moment d'activation spécifié (un état ou un événement) intervient dans le système, Policy Xpress recherche toutes les stratégies qui présentent ce moment d'activation et évalue chaque stratégie en fonction de l'ordre défini.

Remarque : Toute stratégie qui comporte un moment d'activation intervenant dans le système n'est pas forcément exécutée. En effet, des critères de règles évalués ultérieurement dans le processus détermineront son exécution ou sa non-exécution.

Eléments de données

Les éléments de données sont utilisés pour créer des données de stratégies. Une stratégie peut contenir plusieurs éléments de données qui représentent les informations utilisées par la stratégie.

Policy Xpress utilise des modules d'extension flexibles pour rassembler les informations des éléments de données. Chaque module d'extension peut effectuer une petite tâche dédiée. Cependant, plusieurs modules d'extension peuvent être utilisés ensemble pour élaborer des stratégies plus complexes. Comme exemple de module d'extension d'éléments de données, citons un élément d'attribut d'utilisateur. L'objectif de l'élément est de rassembler des informations sur un attribut spécifique qui fait partie du profil de l'utilisateur.

Les éléments de données sont calculés lorsqu'ils sont appelés, c'est-à-dire lorsqu'une règle utilise l'élément de données ou qu'un autre élément nécessitant un calcul utilise l'élément de données comme paramètre.
Par exemple, un élément de données de requête SQL peut récupérer une valeur d'une table, mais il a besoin du service de l'utilisateur pour élaborer la requête. Dans ce cas, l'élément de données de service doit s'exécuter avant l'élément de données de requête SQL, de sorte que la valeur puisse ensuite être utilisée comme paramètre (page 339).

Les champs définissant un élément de données sont les suivants :

Nom

Définit un nom convivial qui décrit l'élément de données. Certains éléments de données sont complexes (par exemple, l'obtention de variables ou la récupération d'informations de la base de données). Veillez donc à choisir un nom significatif pour simplifier la gestion de ces éléments.

Catégorie

Fournit un regroupement d'éléments de données. Ce champ trie les éléments de données et simplifie la sélection.

Type

Spécifie le type d'éléments de données, chacun avec son utilisation propre. Ce champ est basé sur la catégorie sélectionnée.

Fonction

Définit des variations possibles de données identiques. La plupart des éléments de données prennent uniquement en charge la fonction Obtenir.

Par exemple, l'élément de données de l'attribut d'utilisateur possède les fonctions suivantes :

- Obtenir : renvoie les valeurs de l'attribut.
- Valeurs multiples : renvoie True si la valeur est multiple.
- Attribut logique : renvoie True si la valeur est logique.

Description de la fonction

Fournit une description prérenseignée de la fonction. Chaque fonction sélectionnée propose une description différente pour permettre de comprendre son utilisation et les valeurs attendues.

Paramètres

Définit les paramètres transmis à l'élément de données. Les éléments de données sont dynamiques et peuvent effectuer différentes choses en fonction des paramètres. Un élément de données de l'attribut d'utilisateur renvoie différents résultats en fonction de l'attribut sélectionné. L'option de sous-type définit également le nombre de paramètres, leurs noms et les valeurs facultatives le cas échéant.

Vous pouvez ajouter des paramètres supplémentaires si nécessaire. L'exemple de requête SQL accepte deux paramètres requis, à savoir la source de données et la requête elle-même. La requête peut inclure le caractère "?" à remplacer par des valeurs (comme une instruction préparée). L'ajout de paramètres supplémentaires vous permet de définir ces valeurs.

Remarque : Lorsque vous affichez des éléments de données dans Policy Xpress, une colonne est intitulée "En cours d'utilisation". Une coche dans cette colonne signifie que l'élément de données est utilisé par une règle, un paramètre d'action ou comme paramètre pour d'autres éléments de données.

Utilisation de valeurs dynamiques dans les éléments de données ou d'action

Les valeurs dynamiques sont le résultat d'éléments de données calculés et leurs valeurs sont uniquement fixées au moment de l'exécution. Ces valeurs peuvent ensuite être utilisées comme paramètres d'autres éléments de données (qui sont calculés par la suite, en fonction de la priorité).

Pour utiliser une valeur dynamique comme paramètre pour un élément de données

1. Sous l'onglet Données de la stratégie, recherchez le paramètre pour lequel vous souhaitez définir une valeur dynamique.
2. Dans le champ de texte vide, entrez un texte ou sélectionnez la valeur dynamique dans la liste déroulante correspondante.
3. Cliquez sur OK.

Variables

Policy Xpress possède des variables qui sont définies avec des actions et enregistrées comme éléments de données (catégorie Variables). Les variables sont partagées par toutes les stratégies exécutées simultanément, de sorte qu'une variable qui a été définie puisse être utilisée par d'autres stratégies de priorité inférieure.

Par exemple, une variable peut contenir une valeur calculée une fois par une stratégie, puis partagée avec d'autres stratégies, lesquelles n'ont donc plus besoin de la recalculer. La stratégie initiale définit une valeur pour la variable et les stratégies exécutées ultérieurement lisent cette valeur à l'aide d'un élément de données qui possède le nom de la variable comme paramètre.

Une variable peut également être un déclencheur pour d'autres stratégies. Dans ce cas, les stratégies ne sont exécutées que si la stratégie qui les précède a été exécutée.

Règles de saisie

Les règles de saisie définissent les conditions d'exécution d'une stratégie. Ces conditions utilisent les valeurs rassemblées par les éléments de données dans la stratégie.

Une stratégie peut comporter plusieurs règles de saisie, lesquelles peuvent chacune contenir plusieurs conditions. Au moins une règle de saisie doit être respectée, autrement dit *toutes* ses conditions doivent être satisfaites pour que le processus d'une stratégie puisse passer aux règles d'action.

Les champs définissant une règle de saisie sont les suivants :

Nom

Définit un nom convivial pour la règle de saisie.

Description

Détermine la signification de la règle de saisie.

Conditions

Spécifie les critères à respecter.

Remarque : Les conditions d'une règle de saisie sont toujours reliées par un opérateur AND (et).

Informations complémentaires :

Conditions (page 340)

Conditions

Une condition est utilisée dans les règles de saisie et d'action et comprend les composants suivants :

- Données de la stratégie
- Opérateur
- Valeur

Imaginons, par exemple, que vous souhaitez créer une condition qui vérifie si le service d'un utilisateur a été modifié. D'abord, définissez un élément de données Service modifié. Ensuite, dans la condition, sélectionnez l'élément de données Service modifié, définissez l'opérateur sur Egal à et la valeur sur True.

Informations complémentaires :

Règles de saisie (page 339)
Règles d'action (page 340)

Règles d'action

Les règles d'action sont similaires aux règles de saisie sur le plan de la structure, mais se distinguent par leur fonctionnalité. Les règles d'action définissent le moment d'exécution d'une action. Par exemple, si vous voulez qu'une stratégie exécute une action lorsque le service d'un utilisateur est changé en Ventes, créez une règle d'action qui définit quand "Service = Ventes".

Par ailleurs, au lieu de devoir respecter une seule règle de saisie, il peut être nécessaire de satisfaire à plusieurs règles d'action. La règle d'action unique avec la priorité la plus élevée (à savoir 0) est la *seule* utilisée.

Les règles d'action contiennent également une ou plusieurs actions, lesquelles sont divisées en deux groupes : Actions Ajouter et Actions Supprimer.

Les champs définissant une règle d'action sont les suivants :

Nom

Définit un nom convivial pour la règle d'action. Ce nom doit être unique.

Description

Détermine la signification de la règle d'action.

Conditions

Spécifie les critères à respecter.

Priorité

Détermine la règle d'action qui s'exécute, si plusieurs sont respectées. Ce champ permet de définir les actions par défaut. Par exemple, si vous avez plusieurs règles, chacune pour un nom de service, il est possible de définir une valeur par défaut en ajoutant une règle supplémentaire sans condition mais avec une faible priorité (par exemple 10 si toutes les autres ont 5). Si aucune des règles de service sont respectées, le système utilise la valeur par défaut.

Actions Ajouter

Définit une liste d'actions entreprises lorsque la règle est respectée. Par exemple, vous pouvez configurer une règle qui établit que si le service de l'utilisateur correspond à celui configuré dans la condition, un groupe Active Directory spécifique doit être ajouté. Les règles d'action se comportent différemment, en fonction du paramètre Exécuter une fois. Si la stratégie est définie pour être exécutée une seule fois, les actions associées sont exécutées lorsque la règle est respectée pour la première fois. Elles ne sont pas réexécutées lors des correspondances ultérieures avec la règle. Dans l'exemple ci-dessus, le groupe Active Directory n'est ajouté à l'utilisateur qu'une seule fois. Si le paramètre Exécuter une fois n'est pas défini, les actions sont de nouveau exécutées tant que la règle est respectée. Ce champ est essentiel pour l'application de valeurs.

Actions Supprimer

Définit une liste des actions à exécuter lorsque la règle n'est plus respectée. Par exemple, dans l'exemple précédent, un groupe Active Directory a été ajouté à l'utilisateur en fonction du service de ce dernier. Si le service change, l'action de suppression supprime le groupe Active Directory.

Informations complémentaires :

Conditions (page 340)

Actions

Les actions appliquent la logique métier lorsque toutes les décisions sont prises. Le fonctionnement d'une action est semblable à celui d'éléments de données, sauf à la fin. Lorsqu'elle s'exécute, elle effectue une tâche au lieu de renvoyer une valeur.

Remarque : Les actions sont exécutées dans l'ordre dans lequel elles apparaissent dans la console d'utilisateur.

Les champs définissant une action sont les suivants :

Nom d'action

Définit l'objectif de l'action.

Catégorie

Définit un regroupement d'actions. Ce champ trie les actions et simplifie la sélection.

Type et Fonction

Définit le type et la fonction de l'action entreprise.

Remarque : Pour plus d'informations sur le type et la fonction, reportez-vous à la rubrique Données.

Description de la fonction

Fournit une description prérenseignée de la fonction. Chaque fonction sélectionnée propose une description différente pour permettre de comprendre son utilisation et les valeurs attendues.

Paramètres

Définit les paramètres transmis à l'action.

Contrôle des flux

Par défaut, les stratégies sont triées par priorité, puis évaluées une par une. Bien que ce flux s'applique dans presque tous les cas, vous pouvez le changer le cas échéant.

Cette fonctionnalité de modification du flux est représentée par une action qui peut être rattachée à n'importe quelle règle d'action. Les fonctions de modification des flux se situent dans la catégorie Système de l'action.

Important : Agissez avec précaution lorsque vous modifiez les flux de processus. L'utilisation de ces actions peut entraîner une boucle infinie. Par exemple, si vous définissez "Réexécuter la stratégie actuelle" pour une règle d'action sans conditions, la règle sera toujours vraie et la stratégie recommencera sans cesse et ne se fermera jamais.

Les quatre fonctions de modification des flux pouvant être utilisées sont les suivantes :

Arrêter le traitement

Toutes les stratégies consécutives à la stratégie actuelle sont ignorées et Policy Xpress se ferme.
Remarque : Seul Policy Xpress se ferme. Si vous voulez également forcer l'arrêt de CA IdentityMinder, vous pouvez utiliser le module d'extension d'action de type Exception.

Redémarrer toutes les stratégies

Interrompt le traitement du reste des stratégies et retourne au début de la liste. Cette option est utile dans les cas où l'action d'une stratégie a pour conséquence qu'une stratégie précédente qui n'avait pas été exécutée répond à présent aux critères de saisie. Cette stratégie est alors réévaluée.

Réexécuter la stratégie actuelle

La stratégie en cours est à nouveau exécutée. Cette option est utile pour l'itération. Par exemple, la création d'un nom d'utilisateur unique exige qu'une stratégie soit exécutée encore et encore jusqu'à ce qu'elle trouve un nom unique.

Accéder à une stratégie spécifique

Cette action nécessite la sélection d'une stratégie existante. Si cette stratégie est exécutée en même temps que la stratégie actuelle (elle peut l'être avant ou après), Policy Xpress passe à la stratégie sélectionnée. Si la nouvelle stratégie présente une priorité inférieure, toutes les stratégies comprises entre la stratégie actuelle et la stratégie sélectionnée sont ignorées. Si la priorité de la nouvelle stratégie est supérieure, le processus revient en arrière.

Remarque : Etant donné que cette action peut amener Policy Xpress à ignorer certaines stratégies, utilisez ce type d'action avec précaution.

Définition d'objets associés à des comptes

Lors de la création d'une action Ajouter pour définir un objet associé à un compte, par exemple Membre de, un format de relation spécifique est utilisé pour représenter l'objet. Les deux types de formats pouvant représenter l'objet dans CA IdentityMinder sont les suivants.

- Pour représenter des relations simples entre l'objet et le compte, par exemple, des groupes Active Directory :
  `NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server`
- Pour représenter des relations d'association entre l'objet et le compte, par exemple, des rôles SAP :
  `{"validFromDate":"2009\/12\/01","roleName":"SAPRole=SAP_AUDITOR_ADMIN,EndPoint=sap endpoint,Namespace=SAP R3,Domain=im,Server=Server","validToDate":"2009\/12\/31"}`

  Une relation d'association diffère d'une relation simple en ce sens que l'association entre l'objet et le compte comporte des données supplémentaires. Dans l'exemple précédent, les paramètres validFromDate et validToDate ne contiennent que des données liées à l'association entre le compte et le rôle SAP. Les données validFromDate et validToDate n'existent pas au niveau du compte ou de l'objet Rôle.

Pour déterminer le format de la relation, créez un élément de données qui récupère la valeur de l'objet. La valeur retournée correspond au format utilisé dans l'action Ajouter pour définir cet objet.

Exemple : Groupes Active Directory

1. Créez une stratégie Policy Xpress présentant les paramètres suivants.
   - Type de stratégie : Evénement
   - Evénements : Après – Modifier un utilisateur
2. Dans la règle d'action, configurez l'action Ajouter suivante.
   - Catégorie : Attributs
   - Type : Définir les données de compte
   - Fonction : Définir
   - Type de terminal : Active Directory
   - Terminal : *nom_terminal*
   - Nom du compte : *compte*
   - Attribut : Membre de (groupMembership)
   - Valeur : NativeGroup=Administrators,Container=Builtin,Endpoint=*nom_terminal*,Namespace=ActiveDirectory,Domain=im,Server=Server

Avancé

Policy Xpress autorise plusieurs variantes de configuration et interagit également avec des composants externes. En raison de cette flexibilité, des erreurs qui ne sont pas nécessairement des bogues peuvent survenir, comme une source de données mal configurée, une valeur manquante retournée par un élément de données dynamique ou un terminal qui ne répond pas.

Généralement, lorsqu'une erreur se produit, le système arrête le calcul des stratégies pour l'étape en cours. Toutefois, vous pouvez modifier la réponse par défaut aux erreurs, en fonction de la catégorie de ces dernières. Par exemple, si vous possédez une stratégie non critique, vous pouvez définir que le traitement se poursuit en cas d'erreur.

L'onglet Avancé vous permet de modifier les réponses par défaut aux erreurs, le cas échéant.

Remarque : Nous vous recommandons de conserver les paramètres par défaut pour ces réponses ; pour les cas d'utilisation avancés, ils peuvent toutefois être modifiés par stratégie. Par exemple, si vous possédez une stratégie non critique, vous pouvez définir la poursuite du traitement même en cas d'échec de la stratégie.

Les catégories d'erreurs pouvant être configurées sous l'onglet sont les suivantes :

- Validation : résulte de la fourniture d'informations incorrectes à un module d'extension. Ce type d'erreur est signalé avant que l'action soit tentée.
- Environnement : résulte de problèmes au sein de l'environnement, tels qu'un serveur de base de données défaillant pour le module d'extension SQL.
- Autorisé : erreur non critique. Le comportement par défaut pour ce type d'erreur est la poursuite du traitement de la demande, par exemple lorsque l'envoi d'un courriel échoue.

Pour chacune des erreurs précédentes, les options suivantes peuvent être définies :

- Echec de l'événement : arrête l'action en cours. Il s'agit de la valeur par défaut pour la plupart des types d'erreur.
- Echec de la stratégie : arrête la stratégie en cours et toutes les actions associées. Les autres stratégies se poursuivent.
- Ignorer : consigne tous les échecs mais n'arrête pas les actions ni les stratégies.

Chapitre 16: Génération de rapports

Ce chapitre traite des sujets suivants :

Présentation

Dans CA IdentityMinder, vous pouvez exécuter deux types de rapports.

- Rapports sur les clichés : incluent les données de la base de données de clichés, qui contient des informations sur la banque d'objets CA IdentityMinder et sur le magasin d'utilisateurs CA IdentityMinder. Il peut s'agir par exemple d'un rapport sur le profil de l'utilisateur. Vous définissez les données ajoutées à la base de données de clichés à l'aide de définitions de clichés qui spécifient les informations à inclure.
- Rapports non spécifiques aux clichés : incluent des données provenant d'autres sources, telles que la base de données d'audit. Par exemple, Identity Manager inclut des rapports d'audit par défaut. Le nom de ces rapports contient le préfixe "Audit" dans la console d'utilisateur. Bien que CA IdentityMinder inclut par défaut uniquement des rapports d'audit, vous pouvez créer vos propre rapports personnalisés dont les données proviennent d'une source de données, telle que le flux de travaux ou les bases de données de persistance des tâches.

Il est nécessaire de configurer chaque rapport CA IdentityMinder avant de pouvoir l'exécuter. Cette configuration dépend du type de rapport que vous souhaitez exécuter.

Pour les rapports sur les clichés (page 350), procédez comme suit :

1. Créez un fichier de définition de cliché pour définir les données ajoutées à la base de données de clichés.
2. Capturez les données de cliché du rapport.
3. Modifiez la tâche Rapport dans CA IdentityMinder et effectuez les actions ci-dessous.
    a. Association d'une définition de cliché à la tâche
    b. Ajout de l'objet de connexion rptParamConn à la tâche

4. Lancez le rapport en utilisant l'une des méthodes ci-après.
   - Exécution immédiate du rapport
   - Planification du rapport
5. Affichez le rapport dans la console d'utilisateur.

Pour les rapports non spécifiques aux clichés (page 373), procédez comme suit :

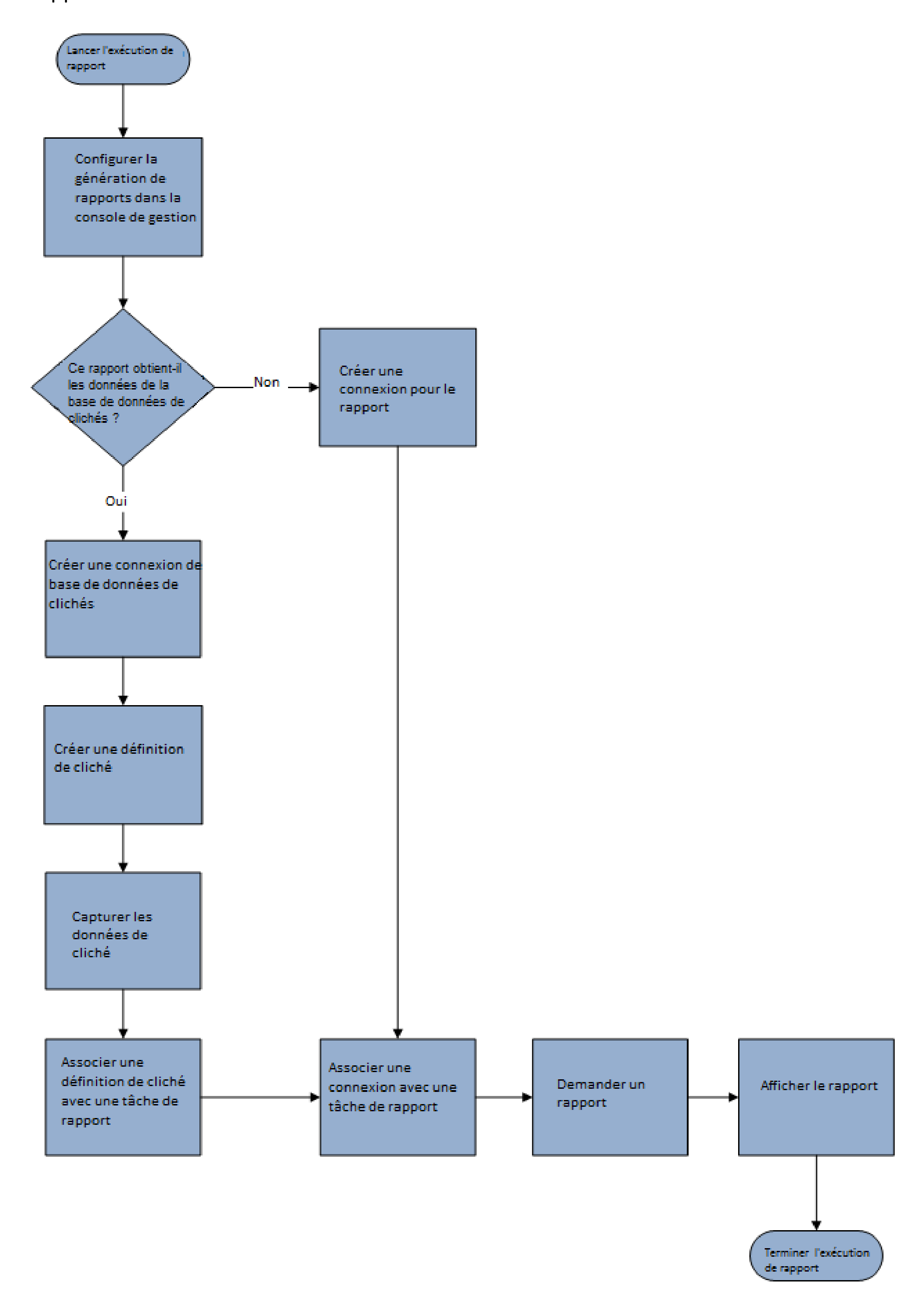
1. Créez un objet de connexion avec les informations de source de données du rapport.
2. Modifiez la tâche Rapport dans CA IdentityMinder et ajoutez l'objet de connexion à la tâche.
3. Lancez le rapport en utilisant l'une des méthodes ci-après.
   - Exécution immédiate du rapport
   - Planification du rapport
4. Affichez le rapport dans la console d'utilisateur.

Une fois la configuration initiale du rapport terminée, vous pouvez demander un rapport dans CA IdentityMinder. Vous pouvez exécuter un rapport immédiatement ou planifier son exécution ultérieure. Vous pouvez également créer une planification récurrente pour votre rapport dans CA IdentityMinder.

Enfin, vous pouvez afficher le rapport dans la console d'utilisateur ou l'exporter dans divers formats.

Processus lié aux rapports

Le graphique suivant illustre le processus requis pour l'exécution et l'affichage de rapports :



Exécution de rapports sur les clichés

Le tableau suivant présente la procédure d'exécution de rapports de base de données de clichés dans CA IdentityMinder.

Etape	Voir
1. Configurer la génération de rapports dans la console de gestion.	Configuration des rapports (page 350)
2. Créer une connexion de la base de données de clichés.	Création d'une connexion de la base de données de clichés (page 351)
3. Créez une définition de cliché.	Création d'une définition de cliché (page 352)
4. (Facultatif) Capturer les données de clichés.	Capture de données de clichés (page 365)
5. Associer une définition de cliché et une connexion à une tâche de génération de rapports.	Association d'une définition de cliché et d'une connexion à une tâche de génération de rapports (page 368)
6. Demander un rapport.	Demande de rapport (page 370)
7. Affichez le rapport.	Affichage du rapport (page 372)

Configuration de la connexion au serveur de rapports

Configurez la connexion entre CA IdentityMinder et le serveur de rapports.

Remarque : Il est recommandé de définir le même fuseau horaire et la même heure sur tous les systèmes impliqués dans la génération de rapports.

Pour configurer la génération de rapports :

1. Dans la console d'utilisateur, cliquez sur Système, Génération de rapports, Connexion au serveur de rapports.
2. Entrez les paramètres du serveur de rapports. Remarque :
   - Nom d'hôte et Port : nom d'hôte et numéro de port du système sur lequel le serveur de rapports est installé.
   - Nom du dossier de rapports : emplacement des rapports CA IdentityMinder par défaut.
   - ID de l'utilisateur : utilisateur créé pour le serveur de rapports.

- Mot de passe : mot de passe de l'utilisateur créé dans le serveur de rapports.
- Connexion sécurisée : sélectionner la case à cocher pour activer la connexion SSL (Secure Sockets Layer) entre CA IdentityMinder et le serveur de rapports.

  Remarque : Avant de sélectionner la case à cocher Connexion sécurisée, vérifiez que vous avez installé le certificat à partir de BOServer. Pour plus d'informations sur la configuration SSL, consultez le chapitre sur l'installation du serveur de rapports dans le *Manuel d'installation*.
- Serveur Web : défini sur Non IIS pour Tomcat.

3. Cliquez sur Tester la connexion pour vérifier la connexion.
4. Cliquez sur Soumettre.

La connexion à la génération de rapports est établie.

Création d'une connexion de la base de données de clichés

CA IdentityMinder doit savoir où exporter les données de clichés. Créez une connexion de base de données de CA IdentityMinder à la base de données de clichés.

Pour créer une connexion de la base de données de clichés :

1. Dans la console d'utilisateur, accédez à Rapports, Tâches de clichés, Gérer la connexion de la base de données de clichés, Créer une base de données de clichés - Connexion.
2. Créez une connexion de la base de données de clichés en complétant tous les champs nécessaires.
3. Cliquez sur Soumettre.

   Une connexion de la base de données de clichés est créée.

Création d'une définition de cliché

Un cliché reflète l'état des objets dans CA IdentityMinder à un moment donné. Ces données de clichés sont utilisées pour créer un rapport. Pour capturer des données d'objet CA IdentityMinder, vous devez créer une définition de cliché qui exporte les données vers la base de données de clichés. A l'aide de la définition de cliché, vous définissez les règles de chargement des utilisateurs, des terminaux, des rôles d'administration, des rôles de provisionnement, des groupes et des organisations.

Procédez comme suit:

1. Dans la console d'utilisateur, accédez à Rapports, Tâches de clichés, Gérer les définitions de clichés, Créer une définition de cliché.
2. Sélectionnez Créer ou Copier un objet de type Cliché.
3. Cliquez sur Ok.
4. Dans l'onglet Profil, remplissez les champs suivants pour créer un profil de définition de cliché :

   Nom de la définition du cliché

   Identifie le nom unique donné à la définition de cliché.

   Description de la définition du cliché

   Affiche toutes les informations supplémentaires pour décrire le cliché.

   Activé

   Spécifie que CA IdentityMinder crée un cliché selon la définition de cliché actuelle à l'heure planifiée.

   Remarque : Si cette option n'est pas sélectionnée, le cliché ne sera pas capturé à l'heure planifiée. De même, la définition de cliché n'est pas répertoriée dans la fenêtre Données de clichés de capture.

   Nombre de clichés conservés

   Spécifie le nombre de clichés conservés dans la base de données de clichés.

   Remarque : Si vous ne spécifiez pas de valeur pour ce champ, CA IdentityMinder stocke un nombre illimité de clichés.

5. Dans l'onglet Stratégies de clichés, sélectionnez les objets associés aux stratégies à exporter.
6. Dans l'onglet Paramètres du rôle, sélectionnez un ou plusieurs composants de rôle et les attributs disponibles que le cliché exportera.

   Remarque : Dans l'onglet Stratégies de clichés, si vous sélectionnez Rôle d'accès, Rôle d'administration ou l'objet Rôle de provisionnement, sélectionnez les attributs dans l'onglet Paramètres du rôle.

7. Dans l'onglet Détails des attributs de l'utilisateur, sélectionnez un ou plusieurs attributs d'utilisateur pour le cliché à exporter.

Remarque : Dans l'onglet Stratégies de clichés, si vous sélectionnez uniquement l'objet Utilisateur, par défaut, tous les attributs d'utilisateur associés aux données sont exportés.

8. Dans l'onglet Attributs du compte de terminal, sélectionnez un ou plusieurs attributs de compte pour un type de terminal.

   Remarque : Pour un type de terminal sélectionné, par défaut, toutes les données associées aux attributs de compte de terminal sont exportées. Pour capturer des données associées à un attribut spécifique, sélectionnez l'attribut approprié. Pour plus d'informations sur la sélection des attributs à exporter pour un type de terminal, consultez la rubrique relative aux rapports par défaut dans le *Manuel de configuration*.

9. (Facultatif) Sélectionnez la case à cocher Exporter les comptes orphelins pour inclure des comptes de terminal sans utilisateur global dans le serveur de provisionnement.

   Remarque : Pour exporter des données de rapport pour les rapports de comptes orphelins, de tendances des comptes non standard et des comptes non standard, sélectionnez l'attribut exceptionAccount et activez la case à cocher Exporter les comptes orphelins.

10. Cliquez sur Soumettre.

    CA IdentityMinder est configuré pour créer des clichés des objets mentionnés dans la définition de cliché.

Après avoir créé une définition de cliché, vous pouvez capturer les données de cliché immédiatement ou planifier l'exportation des données de cliché ultérieurement. La rubrique Capture de données de clichés (page 365) fournit davantage d'informations.

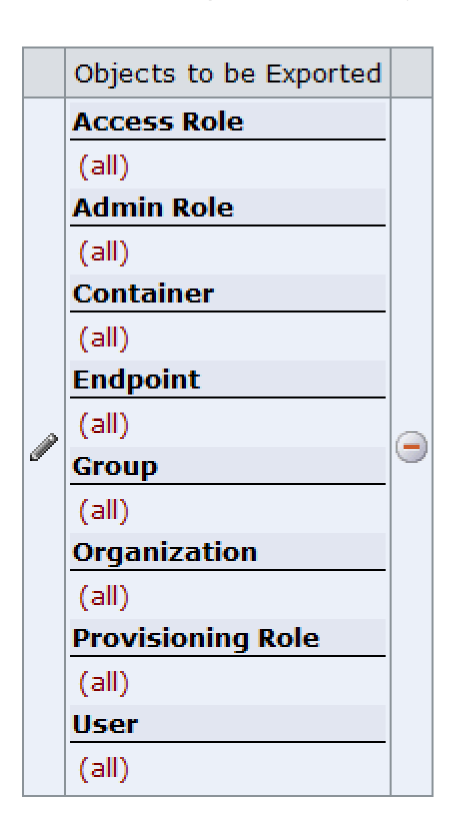
Informations complémentaires :

Onglet Récurrence (page 366)

Exemple : Création d'une définition de cliché pour des données de droits d'utilisateurs

L'exemple suivant illustre le processus de création d'une définition de cliché pour un rapport de droits d'utilisateurs :

1. Dans la console d'utilisateur, accédez à Rapports, Tâches de clichés, Gérer les définitions de clichés, Créer une définition de cliché.
2. Sélectionnez Créer un objet de type Cliché.
3. Entrez le nom de la définition de cliché, la description et le nombre de clichés conservés.
4. Dans l'onglet Définition d'une stratégie de clichés, cliquez sur Ajouter.
5. Dans la liste déroulante, sélectionnez l'utilisateur et sélectionnez Tout. De même, ajoutez Terminal, Rôle de provisionnement, Rôle d'administration, Rôle d'accès, Conteneur, Organisation et Groupe comme illustré dans la fenêtre suivante :



6. Dans l'onglet Paramètres du rôle, sélectionnez toutes les cases à cocher du rôle Utilisateur.
7. Dans l'Onglet attributs de l'utilisateur, sélectionnez les attributs requis dans la liste Valeurs disponibles et déplacez-les vers la liste Valeurs actuelles.
8. Cliquez sur Soumettre.

Fichier XML des paramètres de cliché

Les rapports CA IdentityMinder permettent d'afficher l'état actuel d'un environnement CA IdentityMinder. Vous pouvez utiliser ces informations pour vous assurer de la conformité avec les stratégies métiers internes ou les réglementations externes.

Vous générez des rapports CA IdentityMinder à partir de données de gestion qui décrivent la relation qui existe entre les objets d'un environnement CA IdentityMinder. Voici des exemples de données de gestion :

- Attributs de profil d'un utilisateur
- Liste de rôles contenant une certaine tâche
- Membres d'un rôle ou groupe
- Règles comprenant un rôle

Utilisez le fichier XML des paramètres de cliché approprié pour définir les données de gestion utilisées dans le rapport.

La table suivante répertorie les fichiers XML par défaut et leurs rapports associés :

Fichier XML des paramètres de cliché	Rapport utilisant le fichier XML	Objets exportés par le fichier XML
AccountDetailsReportSnapshot.xml	Rapport sur les détails du compte	■ Objets du rôle de provisionnement ■ Objet du terminal incluant des détails sur le compte
AdministrationReportSnapshot.xml	Rapport d'administration	■ Rôles d'administration, d'accès et de provisionnement avec leurs règles de portée ■ Propriétaires des rôles ■ Administrateurs de rôles ■ Membres avec rôles ■ Tâches affectées à chaque rôle
EndpointAccountsReportSnapshot.xml	Rapport sur les comptes de terminaux	■ Utilisateurs globaux et leurs relations de compte ■ Objet de terminal incluant les détails du terminal avec ses comptes
EndpointDetailsReportSnapshot.xml	Rapport sur les détails du terminal	Objet de terminal incluant les détails du terminal avec ses comptes

Fichier XML des paramètres de cliché	Rapport utilisant le fichier XML	Objets exportés par le fichier XML
NonStandardsAccountsReportSnapshot.xml	Rapport sur les comptes non standard	■ Utilisateurs globaux et leurs relations de compte ■ Objet de terminal incluant les détails du terminal avec ses comptes
NonStandardsAccountsTrendReportSnapshot.xml	Rapport sur les tendances des comptes non standard	■ Utilisateurs globaux et leurs relations de compte ■ Objet de terminal incluant les détails du terminal avec ses comptes
OrphanAccountsReportSnapshot.xml	Rapport sur les comptes orphelins	■ Comptes affectés à [l'utilisateur par défaut] ■ Détails du terminal
PoliciesReportSnapshot.xml	Rapport sur les stratégies	Informations sur toutes les stratégies d'identité d'un environnement
RoleAdministratorsReportSnapshot.xml	Rapport d'administration des rôles	■ Rôles d'administration, d'accès et de provisionnement ■ Administrateurs de rôles
RoleMembersReportSnapshot.xml	Rapport sur les membres avec rôles	■ Rôles d'administration, d'accès et de provisionnement ■ Membres de rôles
RoleOwnersReportSnapshot.xml	Rapport sur les propriétaires des rôles	■ Rôles d'administration, d'accès et de provisionnement ■ Propriétaires des rôles
RolesReportSnapshot.xml	Rapport sur les rôles	■ Rôles d'administration, d'accès et de provisionnement avec leurs règles de portée ■ Propriétaires des rôles ■ Administrateurs de rôles ■ Membres avec rôles ■ Tâches affectées à chaque rôle
TaskRolesReportSnapshot.xml	Rapport sur les rôles des tâches	■ Rôles d'administration, d'accès et de provisionnement ■ Tâches affectées à chaque rôle

Fichier XML des paramètres de cliché	Rapport utilisant le fichier XML	Objets exportés par le fichier XML
UserAccountsReportSnapshot.xml	Rapport sur les comptes d'utilisateurs	■ Utilisateurs globaux et leurs relations de compte ■ Objet de terminal incluant les détails du terminal avec ses comptes
UserEntitlementsReportSnapshot.xml	Rapport sur les droits des utilisateurs	■ Utilisateurs globaux et leurs relations de compte ■ Objet de terminal incluant les détails du terminal avec ses comptes ■ Groupes et membres du groupe ■ Rôles et membres avec rôle
UserPolicySyncStatusReportSnapshot.xml	Rapport sur le statut de synchronisation des stratégies d'utilisateur	■ Utilisateurs globaux et leurs informations d'allocation, de désallocation et de réallocation ■ Détails sur les stratégies d'identité
UserProfileReportSnapshot.xml	Rapport sur le profil de l'utilisateur	■ Détails sur les utilisateurs globaux ■ Détails sur l'organisation
UserRolesReportSnapshot.xml	Rapport sur les rôles d'utilisateurs	Détails sur les utilisateurs globaux et les rôles (d'administration, d'accès et de provisionnement) qui leur sont associés
ExportALLTemplate.xml	Utilisé par tous les rapports	Echantillon XML pour l'exportation des objets sélectionnés (utilisateurs, rôles, groupes, comptes d'utilisateurs et terminaux). Remplacez le texte encadré par les signes ## pour exporter uniquement les valeurs d'objet sélectionnées.

Configuration d'un fichier XML des paramètres de cliché

Pour contrôler les données que CA IdentityMinder exporte, créez un fichier XML des paramètres de cliché. Dans ce fichier, répertoriez les objets à exporter et, éventuellement, spécifiez des critères d'exportation supplémentaires. Dans ce cas, seuls les objets conformes aux critères sont exportés. Par exemple, vous pouvez exporter des informations sur les utilisateurs associés à une certaine valeur d'attribut.

Le fichier XML des paramètres de cliché est au format suivant :

```
<IMRExport>
    <export object="user">
        <where attr="%USER_ID%" satisfy="ANY">
            <value op="EGAL A">abc*</value>
        </where>
        <exportattr attr="%USER_ID%"/>
        <exportattr attr="title"/>
        <exportattr attr="|groups|" />
        <exportattr attr="|roles|" />
        <exportattr attr="|identitypolicystatus|" />
    </export>
</IMRExport>
```

Le fichier XML des paramètres de cliché contient les éléments suivants :

<export>

Spécifie l'objet à exporter. Par exemple, l'élément <export> peut exporter les données de l'utilisateur.

L'élément <export> peut inclure un ou plusieurs éléments <exportattr> et <where>, qui vous permettent d'exporter uniquement les données qui répondent à certains critères. Si aucun élément <exportattr> ou <where> n'est spécifié, toutes les données de l'objet sont exportées.

L'élément <export> possède uniquement le paramètre d'objet.

<where>

Filtre les données qui sont exportées selon des critères spécifiques définis par l'élément <value>. Un élément <where> doit inclure au moins un élément <value>. En outre, vous pouvez spécifier plusieurs éléments <where> pour affiner le filtre (ils agissent alors en tant qu'éléments OU).

Par exemple, vous pouvez utiliser les éléments <where> et <value> pour exporter les tâches pour les rôles activés.

```
<export object="role">
  <where attr="enabled" satisfy="ALL">
    <value op="EGAL A">Yes</value>
  </where>
  <exportattr attr="|tasks|">
</export>
```

Le tableau suivant décrit les paramètres de l'élément <where>.

Paramètre	Description
attr	Spécifie l'attribut à utiliser dans le filtre. Par exemple, si vous spécifiez l'attribut activé, CA IdentityMinder vérifie la valeur de celui-ci pour déterminer s'il est nécessaire d'exporter le rôle.
satisfy	Spécifie si une partie ou la totalité des évaluations de valeur doit être satisfaite pour que l'objet ou les attributs soient exportés. ■ ALL : un attribut ou un objet doit satisfaire à toutes les évaluations de valeur. ■ ANY : un attribut ou un objet doit satisfaire à au moins une évaluation de valeur.

<value>

Définit, dans un élément <where>, la condition à laquelle un attribut ou un objet doit satisfaire pour être exporté. L'élément <value> nécessite le paramètre d'opérateur (op). L'opérateur peut être EGAL A ou CONTIENT.

<exportattr>

Spécifie un attribut spécifique à exporter. Utilisez l'élément <exportattr> pour exporter un sous-ensemble d'attributs pour l'objet en cours d'exportation. Par exemple, vous pouvez utiliser l'élément <exportattr> pour exporter uniquement l'ID d'un utilisateur.

De même, lorsque vous exportez un objet de terminal, vous pouvez utiliser l'élément <exportattr> pour définir les attributs de compte à exporter avec un type de terminal particulier, comme suit.

```
<exportattr objecttype="type_terminal">
<objattr name="description"/>
<objattr name="fullName"/>
<objattr name="lastLogin"/>
</exportattr>
```

L'élément <exportattr> possède le paramètre attr ou objecttype.

<objattr>

Spécifie un attribut de terminal à exporter. Utilisé dans l'élément <exportattr> lorsqu'il s'agit du paramètre objecttype.

Le tableau suivant présente les attributs que vous pouvez utiliser dans un élément <where> ou <exportattr>, par objet.

Objet	Attributs que vous pouvez utiliser dans un élément <where>	Attributs que vous pouvez utiliser dans un élément <exportattr>
role	Vous pouvez définir un filtre sur l'attribut name. name : rôles dont le nom correspond au filtre. roletype : type de rôles qui correspondent au filtre, tels que "accès", "admin" ou "provisionnement".	Vous pouvez exporter les attributs suivants. ■ |tasks| : toutes les tâches associées au rôle. ■ |rules| : toutes les règles de membre, d'administration, de propriété et de portée qui s'appliquent au rôle. ■ |users| : tous les membres, administrateurs et propriétaires du rôle. ■ |rolemembers| : tous les membres du rôle. ■ |roleadmins| : tous les administrateurs du rôle. ■ |roleowners| : tous les propriétaires du rôle.

Objet	Attributs que vous pouvez utiliser dans un élément <where>	Attributs que vous pouvez utiliser dans un élément <exportattr>
user	Tout attribut connu ou physique ou l'un des attributs suivants. ■ |groups| : membres d'un groupe. ■ |roles| : membres d'un rôle. ■ |orgs| : utilisateurs dont les profils existent dans les organisations correspondant au filtre.	Vous pouvez exporter les attributs suivants. ■ |all_attributes| : tous les attributs d'utilisateur disponibles. ■ |groups| : tous les groupes dont l'utilisateur est membre ou administrateur. ■ |roles| : tous les rôles dont l'utilisateur est membre, administrateur ou propriétaire. ■ |identitypolicystatus| : toutes les stratégies d'identité qui s'appliquent à un utilisateur ou à un ensemble d'utilisateurs spécifique. ■ |allocations| : toutes les stratégies qui doivent être appliquées à un utilisateur pour la première fois. ■ |reallocations| : toutes les stratégies à réappliquer à un utilisateur. ■ |deallocations| : toutes les stratégies qui ne s'appliquent plus à un utilisateur, car ce dernier ne remplit plus la condition de ces stratégies.
group	Tout attribut connu ou physique ou l'attribut suivant. |groups| : liste des groupes imbriqués au sein d'un groupe correspondant au filtre.	Vous pouvez exporter tout attribut connu ou physique ou les attributs suivants. ■ |all_attributes| : tous les attributs définis pour l'objet Groupe dans le fichier de configuration d'annuaire (directory.xml). ■ |groups| : tous les groupes imbriqués au sein du groupe. ■ |users| : tous les membres du groupe. ■ |groupadmins| : tous les administrateurs du groupe. ■ |groupmembers| : tous les membres du groupe. ■ |users| : tous les administrateurs et les membres du groupe.

Objet	Attributs que vous pouvez utiliser dans un élément <where>	Attributs que vous pouvez utiliser dans un élément <exportattr>
organization	Tout attribut connu ou physique.	Vous pouvez exporter tout attribut connu ou physique ou les attributs suivants. ■ |all_attributes| : tous les attributs définis pour l'objet Organisation dans le fichier de configuration d'annuaire (directory.xml). ■ |orgs| : toutes les organisations imbriquées au sein de l'organisation. ■ |groups| : tous les groupes de l'organisation. ■ |users| : tous les utilisateurs de l'organisation.

Objet	Attributs que vous pouvez utiliser dans un élément <where>	Attributs que vous pouvez utiliser dans un élément <exportattr>
useraccount	Tout attribut connu ou physique ou l'un des attributs suivants. ■ name : comptes qui correspondent au filtre. ■ |groups| : membres d'un groupe. ■ |roles| : membres d'un rôle. ■ |orgs| : utilisateurs dont les profils existent dans les organisations qui correspondent au filtre. ■ |endpoints| : terminaux qui correspondent au filtre. ■ |endpoint_types| : types de terminaux qui correspondent au filtre. **Remarque :** Seul l'opérateur EGAL A est pris en charge dans l'élément <where> pour les filtres endpoints et endpoint_types.	Vous pouvez exporter n'importe quel attribut spécifique à un compte en indiquant les noms des attributs dans le fichier de mappage de type de terminal (imname) ou en utilisant l'un des attributs suivants. ■ |all_attributes| : tous les attributs d'utilisateur disponibles. ■ |accountdata| : nom du compte, terminal, conteneur, domaine et type. ■ |statistics| : date de création et de modification du compte. ■ |assignmentinfo| : auteur et approbateur du compte et motif. ■ |syncwithroles| : indique si le compte est redondant avec les rôles de provisionnement de l'utilisateur ou pas. ■ |entitlementattributes| : tous les attributs de droit qui existent dans le fichier de mappage. ■ |users| : utilisateurs qui satisfont aux critères du filtre. ■ |groups| : nom convivial d'un groupe. Cette recherche affiche les membres du groupe. ■ |roles| : nom convivial d'un rôle. Cette recherche affiche les membres du rôle. ■ |orgs| : nom convivial d'une organisation. Cette recherche affiche les membres de l'organisation. ■ |allocations| : contient le nom des stratégies qui doivent être affectées à l'utilisateur pour la première fois. ■ |reallocations| : contient le nom des stratégies qui doivent être réaffectées à l'utilisateur. ■ |deallocations| : contient le nom des stratégies dont l'affectation à l'utilisateur doit être annulée. ■ |identitypolicystatus| : déclenche l'inclusion d'affectations, de réaffectations et d'annulations d'affectations pour l'utilisateur.

Objet	Attributs que vous pouvez utiliser dans un élément <where>	Attributs que vous pouvez utiliser dans un élément <exportattr>
endpoint	Tout attribut connu ou physique ou les attributs suivants. ■ name : terminaux conformes au filtre. ■ |accounts| : comptes explorés sur le terminal. **Remarque :** Les objets Utilisateur sont également exportés. ■ |endpoint_types| : informations sur le type de terminal.	Vous pouvez exporter les attributs suivants. ■ |all_attributes| : tous les attributs de terminal disponibles. ■ |endpoint_groups| : groupes du terminal (le cas échéant). ■ |accounts| : tous les comptes du terminal. ■ |accounttemplates| : modèles de compte associés au terminal.
identityPolicySet	Vous pouvez définir un filtre sur l'attribut name. name : ensembles de stratégies d'identité qui correspondent au filtre.	Vous pouvez exporter les attributs suivants. ■ |all_attributes| : tous les ensembles de stratégies, toutes les stratégies et toutes les actions. ■ |identitypolicystatus| : toutes les stratégies d'identité qui s'appliquent à un utilisateur ou à un ensemble d'utilisateurs.
PolicyXpress	Vous pouvez définir un filtre sur l'attribut name. name : stratégies Policy Xpress qui correspondent au filtre.	Tous les attributs associés à l'objet sont exportés.
ReverseNewAccountPolicy	Vous pouvez définir un filtre sur l'attribut name. name : stratégies Inverser la création qui correspondent au filtre.	Tous les attributs associés à l'objet sont exportés.
ReverseModifyAccountPolicy	Vous pouvez définir un filtre sur l'attribut name. name : stratégies Inverser la création qui correspondent au filtre.	Tous les attributs associés à l'objet sont exportés.
Email	Vous pouvez définir un filtre sur l'attribut name. name : stratégies de notification par courriel qui correspondent au filtre.	Tous les attributs associés à l'objet sont exportés.

Objet	Attributs que vous pouvez utiliser dans un élément <where>	Attributs que vous pouvez utiliser dans un élément <exportattr>
BulkTaskDef	Vous pouvez définir un filtre sur l'attribut name. name : définitions de tâches en bloc qui correspondent au filtre.	Tous les attributs associés à l'objet sont exportés.

Gestion des clichés

CA IdentityMinder vous permet d'afficher, de modifier et de supprimer vos définitions de clichés. Lorsque vous affichez ou modifiez une définition de cliché, les onglets Profil et Maintenance s'affichent. L'onglet Maintenance apparaît uniquement après la capture d'un cliché. Dans l'onglet Maintenance, vous pouvez supprimer vos clichés (même ceux dont l'état est Echec).

Pour afficher, modifier ou supprimer une définition de cliché, accédez à Rapports, Tâches de clichés, Gérer les définitions de clichés, puis cliquez sur la tâche à exécuter.

Remarque : Si une définition de cliché est utilisée pour exporter des données vers la base de données de clichés, vous ne pouvez pas la supprimer. Quand vous supprimez une définition de cliché en cours d'utilisation, l'exportation des données vers la base de données de clichés est arrêtée mais la définition de cliché est toujours disponible.

Données de clichés de capture

Si vous souhaitez capturer des données de clichés immédiatement ou planifier l'exportation des données de clichés à une date ultérieure ou selon une planification récurrente, exécutez la tâche Données de clichés de capture. Cette tâche exporte les données immédiatement (en fonction de la définition de cliché) dans la base de données de clichés.

Important : L'exportation des données de clichés peut prendre beaucoup de temps si vous avec une grande quantité de données à exporter. Nous vous recommandons de planifier vos clichés lorsque vous devez exporter un volume important de données.

Pour capturer des données de clichés

1. Dans la console d'utilisateur, accédez à Rapports, Tâches de clichés, Données de clichés de capture.
2. Sélectionnez Exécuter pour exporter les données immédiatement ou Planifier un nouveau job (page 366) pour exporter les données ultérieurement ou selon une planification récurrente.
3. Cliquez sur Suivant.

4. Choisissez une définition de cliché.

5. Cliquez sur Soumettre.

   Les données de clichés sont exportées dans la base de données de clichés.

Remarque : Si la tâche Données de clichés de capture semble trop lente, vous pouvez vérifier sa progression en accédant à l'onglet Système et en cliquant sur Afficher les tâches soumises.

Onglet Récurrence

Utilisez cet onglet pour planifier votre job. Cet onglet comporte les champs suivants.

Exécuter

Permet d'exécuter le job immédiatement.

Planifier un nouveau job

Permet de planifier un nouveau job.

Modifier le job actuel

Spécifie que vous voulez modifier un job existant.

Remarque : Ce champ apparaît uniquement si un job a déjà été planifié pour cette tâche.

Nom du job

Spécifie le nom du job que vous souhaitez créer ou modifier.

Fuseau horaire

Spécifie le fuseau horaire du serveur.

Remarque : Si votre fuseau horaire est différent de celui du serveur, une liste déroulante permet de sélectionner votre fuseau horaire ou celui du serveur lorsque vous planifiez un nouveau job. Vous ne pouvez pas changer le fuseau horaire lorsque vous modifiez un job existant.

Planification quotidienne

Indique que le job se répète régulièrement après un certain nombre de jours.

Tous les (nombre) jours

Définit le nombre de jours s'écoulant entre deux exécutions du job.

Planification hebdomadaire

Spécifie que le job est exécuté un ou plusieurs jours spécifiques de la semaine, à une heure précise.

Jour de la semaine

Spécifie le ou les jours de la semaine où le job est exécuté.

Planification mensuelle

Spécifie un jour de la semaine ou du mois où le job s'exécute selon une base mensuelle.

Planification annuelle

Spécifie un jour de la semaine ou du mois où le job s'exécute selon une base annuelle.

Planification avancée

Spécifie les informations de planification supplémentaires.

Expression Cron

Pour obtenir des informations sur le remplissage de ce champ, reportez-vous à l'adresse suivante :

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Heure d'exécution

Spécifie l'heure, au format 24 heures, à laquelle le job est exécuté. Par exemple, 14:15.

Association d'une définition de cliché à une tâche de génération de rapports

Affectez une définition de cliché à une tâche de génération de rapports de façon à ce que CA IdentityMinder sache quelle définition de cliché utiliser lors de la génération du rapport. Les informations pour les rapports CA IdentityMinder peuvent provenir de plusieurs sources et chaque rapport doit être associé à une source de données spécifique, selon les informations à y afficher.

Pour associer une définition de cliché et une connexion à une tâche de génération de rapports :

1. Dans la console d'utilisateur, sélectionnez Rôles et Tâches, Tâches d'administration, puis Modifier la tâche d'administration.
2. Recherchez la tâche de génération de rapports à laquelle associer une définition de cliché.
3. Accédez à l'onglet Onglets, puis cliquez sur en regard de l'onglet Associer des définitions de clichés.
4. Cliquez sur Ajouter.
5. Recherchez la définition de cliché à associer à la tâche de génération de rapports, puis cliquez sur Sélectionner.

   Lorsque vous associez une définition de cliché à une tâche de génération de rapports, tenez compte de ce qui suit.

   - Un rapport peut être associé à une ou plusieurs définitions de clichés.
   - Une définition de cliché peut être associée à plusieurs rapports.
   - Plusieurs clichés associés à une tâche de génération de rapport unique ne peuvent pas utiliser le même intervalle de récurrence.
6. Cliquez sur Ok.
7. Accédez à l'onglet Rechercher, puis cliquez sur Parcourir pour localiser les fenêtres de recherche.
8. Modifiez la fenêtre de recherche pour la tâche de génération de rapports, puis sélectionnez rptParamConn sous Objet de connexion pour le rapport.
9. Cliquez sur Ok.
10. Cliquez sur Sélectionner.
11. Cliquez sur Soumettre.

Configuration de l'administrateur entrant

La synchronisation entrante maintient CA IdentityMinder à jour et applique les modifications appliquées à l'annuaire de provisionnement.

Pour configurer l'environnement CA IdentityMinder pour le serveur de provisionnement, vous devez créer un compte d'utilisateur CA IdentityMinder en tant qu'administrateur entrant pour utiliser la synchronisation entrante.

Procédez comme suit :

1. Connectez-vous à l'environnement CA IdentityMinder avec le rôle Gestionnaire du système.
2. Cliquez sur Utilisateurs, Gérer les utilisateurs, Créer un utilisateur et créez un utilisateur. Par exemple, utilisateur entrant.
3. Cliquez sur Rôles d'administration, Modifier le rôle et sélectionnez un rôle qui contient les tâches que vous utilisez pour la synchronisation.
   - Provisionnement de la création d'utilisateur
   - Provisionnement de l'activation/désactivation d'utilisateur
   - Provisionnement de la modification d'utilisateur

   Remarque : Si vous n'avez pas modifié les tâches de synchronisation par défaut, utilisez le rôle Provisionnement du gestionnaire de synchronisations.
4. Cliquez sur l'onglet Membres, ajoutez une stratégie de membre qui inclut :
   - Une règle de membre indiquant que l'utilisateur remplit l'exigence. Par exemple, ID utilisateur = utilisateur entrant.
   - Une règle de portée fournissant l'accès à tous les utilisateurs affectés par les modification de l'annuaire de provisionnement déclenchant la synchronisation entrante.
5. Dans la console de gestion :
   a. Sélectionnez l'environnement.
   b. Sélectionnez Advanced Settings, Provisioning.
   c. Remplissez le champ Organization for Creating Inbound Users si le répertoire CA IdentityMinder inclut une organisation.

      Remarque : Cette organisation contient les utilisateurs créés lors de la synchronisation entrante.
   d. Remplissez le champ Inbound Administrator en indiquant l'ID de l'utilisateur que vous avez créé lors de l'étape 2.
   e. Cliquez sur Validate (Valider) pour confirmer que l'ID d'utilisateur est accepté.

      Remarque : Si nécessaire, vous pouvez modifier d'autres champs dans la fenêtre. Pour plus d'informations sur chaque champ, cliquez sur le bouton Aide dans la fenêtre.

Vous avez terminé de configurer l'administrateur entrant.

Demande de rapport

Pour afficher un rapport, demandez-le à un utilisateur avec des droits d'administration de rapports. L'approbation est requise, car l'exécution de certains rapports peut requérir un long délai ou des ressources système importantes. Si votre demande de rapport requiert une approbation, le système envoie une alerte par courriel.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur avec des droits d'utilisateur pour les tâches de rapport.
2. Sélectionnez Rapports, Tâches de génération de rapports, Demander un rapport.

   Une liste de rapports s'affiche.
3. Sélectionnez le rapport que vous voulez demander.

   Une fenêtre de paramètres s'affiche.

   Entrez les informations de paramètres requises.

   Remarque : Si vous exécutez un rapport sur les clichés et qu'aucun cliché n'est disponible pour ce rapport, vous devez commencer par capturer un cliché.

   - Certains rapports affichent le statut du système spécifique pour un point dans le temps. Lorsque vous demandez ce type du rapport, vous sélectionnez un point dans le temps pour lequel vous voulez afficher les données de rapport. Ce point dans le temps représente un *cliché*.

     Remarque : Les dates et heures de cliché que vous pouvez choisir sont prédéterminées. Généralement, l'administrateur système, ou un autre utilisateur disposant de droits d'administration de rapport, se charge de la configuration des clichés. Si aucun cliché n'est disponible pour le rapport que vous voulez demander, contactez l'administrateur système.
   - Certains rapports indiquent l'activité pour une période donnée. Les titres de ces rapports commencent généralement par *Audit*. Lorsque vous demandez ce type du rapport, vous spécifiez une période pour laquelle vous voulez afficher les données de rapport. Par exemple, vous pouvez exécuter le rapport Audit - Rapport sur la réinitialisation du mot de passe pour les 30 derniers jours.

4. Cliquez sur Planifier un rapport et sélectionnez une planification pour votre rapport.

   Maintenant

   Spécifie que le rapport est exécuté immédiatement.

   Une fois

   Spécifie que le rapport s'exécute une fois, pendant une période spécifique. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

   Remarque : Vous pouvez sélectionner cette option si le rapport que vous demandez requiert une grande quantité de données. Pour conserver les ressources système, choisissez une période plus creuse du système.

5. Cliquez sur Soumettre.

   La demande de rapport est soumise. Selon la configuration de votre environnement, la demande s'exécute immédiatement ou suite à l'approbation d'un administrateur.

   Généralement, un administrateur système ou un autre utilisateur avec des droits d'administration de rapports doit approuver une demande de rapport avant que le système ne la réalise. L'approbation est requise, car l'exécution de certains rapports peut requérir un long délai ou des ressources système importantes. Si votre demande de rapport requiert une approbation, vous recevrez une alerte par courriel.

Informations complémentaires

Planificateur de rapports (page 377)

Planificateur de rapports

L'exécution de certains rapports peut prendre beaucoup de temps ou vous souhaitez peut-être afficher le même rapport plusieurs fois sans devoir l'exécuter à chaque fois que vous l'affichez. Le planificateur de rapports permet de planifier la génération automatique d'un rapport ultérieurement. Une fois le rapport généré, vous pouvez l'afficher à plusieurs reprises sans l'exécuter à nouveau.

Vous pouvez utiliser les options suivantes pour planifier des rapports. Selon l'option de planification que vous sélectionnez, CA IdentityMinder affiche des options supplémentaires.

Maintenant

Spécifie que le rapport est exécuté immédiatement.

Une fois

Spécifie que le rapport est exécuté une seule fois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

Gestion des planifications de récurrence des rapports

CA IdentityMinder vous permet d'afficher, de modifier et de supprimer vos planifications de récurrence des rapports.

Pour afficher, modifier ou supprimer une planification de récurrence des rapports, accédez à Rapports, Tâches de génération de rapports, Gérer les planifications de récurrence des rapports, puis cliquez sur la tâche à exécuter.

Remarque : Si vous modifiez une planification de récurrence des rapports, le champ Prochaine exécution est mis à jour uniquement après l'achèvement de la dernière instance de rapport planifiée. Par exemple, si vous planifiez l'exécution quotidienne d'un rapport, la planification de récurrence des rapports affiche des informations sur la date d'exécution de la prochaine instance, par exemple le lendemain à 10 h 00. Si vous définissez la planification de récurrence des rapports sur Tous les mois au lieu de Tous les jours, le serveur de rapports ne met pas à jour immédiatement la prochaine exécution. La planification de récurrence des rapports indique toujours que la prochaine instance sera exécutée le lendemain à 10 h 00. A la fin de cette instance de rapport quotidienne, la prochaine exécution est mise à jour pour refléter la nouvelle planification mensuelle.

Affichage du rapport

Selon la configuration de votre environnement, un rapport s'affiche lorsqu'un administrateur approuve la demande pour ce rapport. Si votre demande de rapport est en attente d'approbation, vous recevrez une alerte par courriel. Le rapport que vous voulez afficher apparaîtra dans la liste de recherche uniquement lorsqu'il sera approuvé.

Procédez comme suit:

1. Dans la console d'utilisateur, accédez à Rapports, Tâches de génération de rapports, puis cliquez sur Afficher mes rapports.
2. Recherchez le rapport à afficher.

   Les rapports de récurrence et les instances de rapports à la demande s'affichent.
3. Sélectionnez le rapport à afficher.

   Remarque : Pour afficher des rapports dans CA IdentityMinder à l'aide de la tâche Afficher mes rapports, activez les cookies de session tiers dans votre navigateur.
4. (Facultatif) Cliquez sur Exporter ce rapport (coin gauche supérieur) pour exporter le rapport dans les formats suivants :
   - Crystal Report
   - Excel
   - PDF

Le rapport personnalisé est généré.

Exécution de rapports non spécifiques aux clichés

Le tableau suivant présente la procédure d'exécution de rapports non spécifiques aux clichés (tels que des rapports d'audit) dans CA IdentityMinder.

Etape	**Voir**
1. Configurer la génération de rapports dans la console de gestion.	Configuration des rapports
2. Créer une connexion JDBC pour la tâche de génération de rapports.	Création d'une connexion pour le rapport
3. Associer une connexion à la tâche de génération de rapports.	Association d'une connexion à une tâche de génération de rapports (Reportez-vous à la définition à la page 369)
4. Demander un rapport.	Demande de rapport
5. Affichez le rapport.	Affichage du rapport (page 372)

Configuration de la connexion au serveur de rapports

Configurez la connexion entre CA IdentityMinder et le serveur de rapports.

Remarque : Il est recommandé de définir le même fuseau horaire et la même heure sur tous les systèmes impliqués dans la génération de rapports.

Pour configurer la génération de rapports :

1. Dans la console d'utilisateur, cliquez sur Système, Génération de rapports, Connexion au serveur de rapports.
2. Entrez les paramètres du serveur de rapports. Remarque :
   - Nom d'hôte et Port : nom d'hôte et numéro de port du système sur lequel le serveur de rapports est installé.
   - Nom du dossier de rapports : emplacement des rapports CA IdentityMinder par défaut.
   - ID de l'utilisateur : utilisateur créé pour le serveur de rapports.

- Mot de passe : mot de passe de l'utilisateur créé dans le serveur de rapports.
- Connexion sécurisée : sélectionner la case à cocher pour activer la connexion SSL (Secure Sockets Layer) entre CA IdentityMinder et le serveur de rapports.

  Remarque : Avant de sélectionner la case à cocher Connexion sécurisée, vérifiez que vous avez installé le certificat à partir de BOServer. Pour plus d'informations sur la configuration SSL, consultez le chapitre sur l'installation du serveur de rapports dans le *Manuel d'installation*.
- Serveur Web : défini sur Non IIS pour Tomcat.

3. Cliquez sur Tester la connexion pour vérifier la connexion.
4. Cliquez sur Soumettre.

La connexion à la génération de rapports est établie.

Création d'une connexion pour le rapport

Les informations incluses dans les rapports CA IdentityMinder peuvent provenir de plusieurs sources. Pour spécifier les détails de connexion à une autre source de données pour le rapport, créez une connexion JDBC dans CA IdentityMinder.

Pour créer une connexion JDBC :

1. Dans la console d'utilisateur, accédez à Système, Gestion des connexions JDBC, Créer une connexion JDBC.
2. Créez un objet de connexion ou choisissez un objet de connexion basé sur une source de données JNDI.
3. Renseignez tous les champs nécessaires, puis cliquez sur Soumettre.

   Une connexion JDBC est créée.

Important : Il est *déconseillé* d'utiliser la base de données de la banque d'objets CA IdentityMinder pour la génération de rapports.

Association d'une connexion à une tâche de génération de rapports

Les informations des rapports CA IdentityMinder peuvent provenir de plusieurs sources et chaque rapport doit être associé à une source de données spécifique, selon les informations à y afficher.

Pour associer une connexion à une tâche de génération de rapports :

1. Dans la console d'utilisateur, sélectionnez Rôles et Tâches, Tâches d'administration, puis Modifier la tâche d'administration.
2. Recherchez la tâche de génération de rapports à laquelle associer une connexion.
3. Accédez à l'onglet Rechercher, puis cliquez sur Parcourir pour localiser les fenêtres de recherche.
4. Modifiez la fenêtre de recherche pour la tâche de génération de rapports, puis sélectionnez une connexion sous Objet de connexion pour le rapport.
5. Cliquez sur Ok.
6. Cliquez sur Sélectionner.
7. Cliquez sur Soumettre.

Demande de rapport

Pour afficher un rapport, demandez-le à un utilisateur avec des droits d'administration de rapports. L'approbation est requise, car l'exécution de certains rapports peut requérir un long délai ou des ressources système importantes. Si votre demande de rapport requiert une approbation, le système envoie une alerte par courriel.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur avec des droits d'utilisateur pour les tâches de rapport.
2. Sélectionnez Rapports, Tâches de génération de rapports, Demander un rapport.

   Une liste de rapports s'affiche.
3. Sélectionnez le rapport que vous voulez demander.

   Une fenêtre de paramètres s’affiche.

Entrez les informations de paramètres requises.

Remarque : Si vous exécutez un rapport sur les clichés et qu'aucun cliché n'est disponible pour ce rapport, vous devez commencer par capturer un cliché.

- Certains rapports affichent le statut du système spécifique pour un point dans le temps. Lorsque vous demandez ce type du rapport, vous sélectionnez un point dans le temps pour lequel vous voulez afficher les données de rapport. Ce point dans le temps représente un *cliché*.

  Remarque : Les dates et heures de cliché que vous pouvez choisir sont prédéterminées. Généralement, l'administrateur système, ou un autre utilisateur disposant de droits d'administration de rapport, se charge de la configuration des clichés. Si aucun cliché n'est disponible pour le rapport que vous voulez demander, contactez l'administrateur système.

- Certains rapports indiquent l'activité pour une période donnée. Les titres de ces rapports commencent généralement par *Audit*. Lorsque vous demandez ce type du rapport, vous spécifiez une période pour laquelle vous voulez afficher les données de rapport. Par exemple, vous pouvez exécuter le rapport Audit - Rapport sur la réinitialisation du mot de passe pour les 30 derniers jours.

4. Cliquez sur Planifier un rapport et sélectionnez une planification pour votre rapport.

   Maintenant

   Spécifie que le rapport est exécuté immédiatement.

   Une fois

   Spécifie que le rapport s'exécute une fois, pendant une période spécifique. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

   Remarque : Vous pouvez sélectionner cette option si le rapport que vous demandez requiert une grande quantité de données. Pour conserver les ressources système, choisissez une période plus creuse du système.

5. Cliquez sur Soumettre.

   La demande de rapport est soumise. Selon la configuration de votre environnement, la demande s'exécute immédiatement ou suite à l'approbation d'un administrateur.

   Généralement, un administrateur système ou un autre utilisateur avec des droits d'administration de rapports doit approuver une demande de rapport avant que le système ne la réalise. L'approbation est requise, car l'exécution de certains rapports peut requérir un long délai ou des ressources système importantes. Si votre demande de rapport requiert une approbation, vous recevrez une alerte par courriel.

Informations complémentaires

Planificateur de rapports (page 377)

Planificateur de rapports

L'exécution de certains rapports peut prendre beaucoup de temps ou vous souhaitez peut-être afficher le même rapport plusieurs fois sans devoir l'exécuter à chaque fois que vous l'affichez. Le planificateur de rapports permet de planifier la génération automatique d'un rapport ultérieurement. Une fois le rapport généré, vous pouvez l'afficher à plusieurs reprises sans l'exécuter à nouveau.

Vous pouvez utiliser les options suivantes pour planifier des rapports. Selon l'option de planification que vous sélectionnez, CA IdentityMinder affiche des options supplémentaires.

Maintenant

Spécifie que le rapport est exécuté immédiatement.

Une fois

Spécifie que le rapport est exécuté une seule fois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

Remarque : Pour accéder aux options de récurrence d'un rapport, sélectionnez Activer l'option de récurrence dans l'onglet Planificateur du serveur de rapports.

(Rapport d'audit uniquement) Toutes les heures

Spécifie que le rapport est généré à l'heure de début, puis toutes les n heures par la suite ; n indiquant un intervalle entre les rapports successifs. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin et l'intervalle entre deux rapports successifs.

(Rapport d'audit uniquement) Tous les jours

Spécifie que le rapport est généré à l'heure de début, puis toutes les n jours par la suite ; n indiquant un intervalle entre les rapports successifs. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin et l'intervalle entre deux rapports successifs.

(Rapport d'audit uniquement) Toutes les semaines

Spécifie que le rapport est généré toutes les semaines le jour sélectionné à compter de la date de début. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Tous les mois

Spécifie que le rapport est généré tous les mois à compter de la date de début, puis toutes les n mois par la suite. "n" désigne l'intervalle entre deux rapports consécutifs. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin et l'intervalle entre deux rapports successifs.

(Rapport d'audit uniquement) Exécuter le rapport à une date précise du mois

Spécifie que le rapport est généré le jour précis que vous avez indiqué dans le mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Premier lundi

Spécifie que le rapport est généré tous les premiers lundis de chaque mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Dernier jour du mois

Spécifie que le rapport est généré le dernier jour du mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport.

(Rapport d'audit uniquement) Un jour et une semaine spécifiques de chaque mois

Spécifie que le rapport est généré le jour précis de la semaine précise de chaque mois. Sélectionnez les dates de début et de fin, ainsi que les heures de début et de fin pour la génération du rapport. Par exemple, vous pouvez générer un rapport le vendredi de la 3e semaine de chaque mois.

Gestion des planifications de récurrence des rapports

CA IdentityMinder vous permet d'afficher, de modifier et de supprimer vos planifications de récurrence des rapports.

Pour afficher, modifier ou supprimer une planification de récurrence des rapports, accédez à Rapports, Tâches de génération de rapports, Gérer les planifications de récurrence des rapports, puis cliquez sur la tâche à exécuter.

Remarque : Si vous modifiez une planification de récurrence des rapports, le champ Prochaine exécution est mis à jour uniquement après l'achèvement de la dernière instance de rapport planifiée. Par exemple, si vous planifiez l'exécution quotidienne d'un rapport, la planification de récurrence des rapports affiche des informations sur la date d'exécution de la prochaine instance, par exemple le lendemain à 10 h 00. Si vous définissez la planification de récurrence des rapports sur Tous les mois au lieu de Tous les jours, le serveur de rapports ne met pas à jour immédiatement la prochaine exécution. La planification de récurrence des rapports indique toujours que la prochaine instance sera exécutée le lendemain à 10 h 00. A la fin de cette instance de rapport quotidienne, la prochaine exécution est mise à jour pour refléter la nouvelle planification mensuelle.

Affichage du rapport

Selon la configuration de votre environnement, un rapport s'affiche lorsqu'un administrateur approuve la demande pour ce rapport. Si votre demande de rapport est en attente d'approbation, vous recevrez une alerte par courriel. Le rapport que vous voulez afficher apparaîtra dans la liste de recherche uniquement lorsqu'il sera approuvé.

Procédez comme suit:

1. Dans la console d'utilisateur, accédez à Rapports, Tâches de génération de rapports, puis cliquez sur Afficher mes rapports.
2. Recherchez le rapport à afficher.

   Les rapports de récurrence et les instances de rapports à la demande s'affichent.
3. Sélectionnez le rapport à afficher.

   Remarque : Pour afficher des rapports dans CA IdentityMinder à l'aide de la tâche Afficher mes rapports, activez les cookies de session tiers dans votre navigateur.
4. (Facultatif) Cliquez sur Exporter ce rapport (coin gauche supérieur) pour exporter le rapport dans les formats suivants :
   - Crystal Report
   - Excel
   - PDF

Le rapport personnalisé est généré.

Définir les options de génération de rapports

Configurez le nombre d'instances de rapport qu'un utilisateur peut générer pour un rapport spécifique.

Pour modifier les options de création de rapport.

1. Sélectionnez Rapports, Tâches de génération de rapports, Définir les options de génération de rapports.

   CA IdentityMinder se connecte au serveur de rapports IAM et extrait la liste de tous les rapports.

2. Choisissez un rapport et cliquez sur Modifier.

   Le volet des rapports apparaît.

3. Modifiez les champs suivants :

   Nom

   Précise le nom d'affichage pour le rapport sélectionné.

   Nombre d'instances

   Précise le nombre d'instances autorisées pouvant être générées par un utilisateur pour ce rapport.

4. Cliquez sur Ok.

   Les attributs du rapport sont modifiés.

Création et exécution de rapports personnalisés

CA IdentityMinder permet de créer et de personnaliser des rapports adaptés aux besoins de votre entreprise.

Le tableau suivant présente la procédure de création de rapports personnalisés dans CA IdentityMinder :

Etape	Voir
1. Création d'un rapport à l'aide de Crystal Reports Developer	Création d'un rapport à l'aide de Crystal Reports (page 381)
2. Création du fichier XML des paramètres du rapport	Création du fichier XML des paramètres du rapport (page 381)
3. Chargement du rapport et du fichier XML des paramètres du rapport vers le serveur de rapports CA	Chargement du rapport et du fichier XML des paramètres du rapport (page 386)
4. Création de la tâche de rapport	Création de la tâche de rapport (page 387)

Etape	Voir
5. Exécution du rapport	Exécution de rapports sur les clichés (page 350) Exécution de rapports non spécifiques aux clichés (page 373)

Création d'un rapport à l'aide de Crystal Reports

CA IdentityMinder permet de créer vos propres rapports personnalisés pour répondre aux besoins de votre entreprise. Pour utiliser des rapports personnalisés dans CA IdentityMinder, créez un rapport (fichier RPT) à l'aide de Crystal Reports Developer. Pour plus d'informations sur la procédure à suivre pour la création d'un rapport à l'aide de Crystal Reports, consultez la documentation Crystal Reports.

Important : Si vous devez référencer le schéma CA IdentityMinder pour créer des rapports personnalisés, le schéma de base de données CA IdentityMinder se trouve à l'emplacement suivant :

<chemin_installation>\db\objectstore

Création du fichier XML des paramètres du rapport

Dans CA IdentityMinder, les rapports disposent de leur propre fenêtre de recherche, de sorte qu'un utilisateur puisse saisir ou sélectionner des données requises lors de la génération d'un rapport. Un paramètre correspond à l'un des champs d'un rapport que vous pouvez utiliser pour filtrer des rapports. Vous pouvez générer un rapport en filtrant les données à l'aide de paramètres. Afin de permettre la personnalisation de la fenêtre de recherche de rapports (fichiers RPT), chacun d'eux est associé à un fichier XML de paramètres de rapport.

Remarque : Vous aurez besoin d'un fichier XML de paramètres de rapport uniquement si le rapport interroge les attributs compris dans l'objet.

Important : Le fichier XML des paramètres du rapport doit porter le même nom que le rapport (fichier RPT) et l'extension .xml. Par exemple, si vous chargez un rapport appelé test1.rpt dans le serveur de rapports, votre fichier XML doit être nommé test1.xml.

Le fichier XML des paramètres de rapport contient les éléments suivants :

<product>

Identifie le produit pour lequel les paramètres sont utilisés. Vous pouvez créer différents paramètres pour plusieurs produits à l'aide du même fichier XML de paramètres.

<screen>

Définit les paramètres qui seront affichés dans une fenêtre. Vous pouvez utiliser l'élément screen (fenêtre) pour établir un lien entre les paramètres et une fenêtre spécifique. De type alphanumérique, l'ID de fenêtre est unique et permet d'identifier les fenêtres et leurs paramètres.

<parameters>

Spécifie la collection de paramètres d'une fenêtre.

<param>

Définit l'élément parameter (paramètre) qui transmet des données spécifiques au rapport. Les attributs suivants sont utilisés dans l'élément <param> :

id

Définit le paramètre dans le rapport à associer.

Remarque : Il doit porter le même nom que le paramètre dans Crystal Reports.

name

Ce champ n'est actuellement pas utilisé par CA IdentityMinder. Définissez cet attribut sur la même valeur que l'ID.

displaytext

Spécifie le texte convivial à afficher pour le paramètre dans la fenêtre.

type

Définit le type de paramètre. L'affichage de la fenêtre change en fonction de cet attribut. Les types de paramètre pris en charge sont les suivants :

- **Zone de texte**

  Exemple : <param id="param1" displaytext="First Name" name="param1" type="string"/>

- **Date et heure**

  Exemple : <param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>

  <param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>

  <param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>

- **Liste déroulante**

  Exemple : <param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>

- **Zone de liste**

  Exemple : <param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>

- **Zone de boutons radio**

  Exemple : <param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>

  <param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>

  <param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>

- **Case à cocher**

  Exemple : <param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>

row

Définit le nombre de lignes visibles dans une zone de liste.

Par défaut : 5

default

Définit la valeur par défaut affichée dans la fenêtre d'un paramètre spécifique. Vous pouvez utiliser cet attribut avec les types chaîne, zone de liste et liste déroulante.

SQL

Vous pouvez définir des requêtes SQL dans une zone de liste ou une liste déroulante du fichier XML des paramètres de rapport. Pour utiliser SQL dans le paramètre de liste déroulante ou de zone de liste, indiquez une instruction SQL valide dans l'attribut SQL.

Exemple :

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'S%/>
```

Dans l'exemple ci-dessus, tous les noms d'utilisateurs dont le prénom commence par un S figureront dans le rapport.

Toutefois, cette condition de prénom commençant par un S est statique. Elle n'est donc pas suffisamment flexible pour qu'un utilisateur charge la valeur en fonction de la valeur de paramètre saisie dans l'une des précédentes fenêtres, utilisée dans le même groupe de paramètres de rapport. Pour utiliser une valeur précédemment saisie dans une autre fenêtre, vous pouvez ajouter ##<parameter id>## à l'instruction SQL.

Par exemple, vous disposez d'un paramètre contenant id=User, de type chaîne :

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>
```

Vous voulez utiliser la valeur entrée de ce paramètre dans SQL, l'instruction SQL devra alors se présenter comme suit :

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname like
'##User##'/>
```

CA IdentityMinder remplacera ##User## par la valeur saisie pour le paramètre avec id=User.

Remarque : La valeur du paramètre qui doit être remplacée ne peut pas figurer dans la même fenêtre que le paramètre SQL. Par exemple, si lstlastname2 est dans la fenêtre 3, le paramètre User doit être dans l'une des fenêtres précédentes.

Beans Java

Si l'utilisation de SQL n'est pas appropriée, vous pouvez utiliser des beans Java pour calculer des valeurs et indiquer la liste de paires <clé, valeur> à CA IdentityMinder. Les beans Java doivent être placés dans le Classpath de CA IdentityMinder.

Exemple :

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2"
type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

Dans l'exemple ci-dessus, TestDataCollector récupère lui-même les valeurs et envoie les données pour la liste déroulante au rapport. Les paires <clé, valeur> sont séparées par %1F.

Veillez à ce que le bean Java se trouve dans le répertoire iam_im.ear\custom.

Remarque : Pour plus d'informations sur l'implémentation des beans Java, reportez-vous à la documentation de BusinessObjects.

Littéraux de chaîne

Pour représenter le plus simplement les valeurs de paramètres d'une liste ou d'une zone déroulante, utilisez des littéraux de chaîne. La valeur clé sera délimitée par %1F et chaque paire <clé, valeur> sera séparée par %1E.

Exemple :

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown"
default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

Paramètres masqués

Les paramètres masqués permettent de transférer des données confidentielles, telles qu'un mot de passe, dans le contexte du rapport. Les données masquées peuvent être utilisées par le rapport, par SQL ou par le bean Java pour traiter la logique métier sans les connaissances de l'utilisateur.

Exemple :

```
<param id="city" displaytext="User1" name="city" hidden="true" type="string"
class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

Dans l'exemple ci-dessus, la valeur du paramètre city (ville) est traitée par le bean Java TestDataCollector, mais n'est pas visible par l'utilisateur.

Veillez à ce que le bean Java se trouve dans le répertoire iam_im\custom.

Exemple de fichier XML de paramètres de rapport

Voici un exemple de fichier XML de paramètres de rapport :

```
<?xml version="1.0" encoding="UTF-8"?>
<product xmlns="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsi="http://www.example.org/Parameters"
xsi:schemaLocation="http://www.example.org/Parameters
../../../reporting/src/com/ca/ims/reporting/utils/Parameters.xsd ">
<screen id="1">
<parameters>
<param id="param1" displaytext="User" name="User" type="string"/>
</parameters>
</screen>
<screen id="Test">
<parameters>
<param id="Test" displaytext="Test" name="Test" type="sqlstr"
conn_id="rptParamConn"
multiselect="true" rows="3" sql="select CUSTOMERID, CONTACTNAME from customers where
customerid like '##param1##'" />
</parameters>
</screen>
</product>
```

Chargement du rapport et du fichier XML des paramètres du rapport

Une fois le rapport (RPT) et le fichier XML des paramètres du rapport correspondant créés, chargez les deux fichiers dans le serveur de rapports CA (BusinessObjects).

Pour charger un rapport et le fichier XML des paramètres du rapport :

1. Connectez-vous à la console de gestion centrale BusinessObjects.
2. Cliquez sur Folders (Dossiers).
3. Sélectionnez le dossier IM Reports (Rapports IM).
4. Cliquez sur New Object (Nouvel objet) et vérifiez que le type d'objet est Crystal Reports.
5. Accédez au nouveau rapport (RPT) créé.
6. Vérifiez que le dossier de rapports IM est sélectionné pour l'enregistrement du rapport.
7. Cliquez sur Soumettre.
8. Dans le coin supérieur gauche, cliquez sur IM Reports (Rapports IM).
9. Cliquez sur New Object (Nouvel objet) et vérifiez que le type d'objet est Texte.
10. Accédez au fichier XML des paramètres du rapport créé.

11. Vérifiez que le dossier de rapports IM est sélectionné pour l'enregistrement du rapport.
12. Cliquez sur Soumettre.
13. Accédez au dossier de rapports IM et vérifiez que les deux nouveaux fichiers sont disponibles.

Création de la tâche de rapport

Les tâches de rapport sont utilisées pour créer, gérer, afficher et supprimer les modèles des rapports générés dans la console d'utilisateur. Le processus de création d'une tâche de rapport est similaire à celui de la création d'une tâche d'administrateur dans CA IdentityMinder.

Pour créer une tâche de rapports :

1. Dans la console d'utilisateur, accédez à Rôles et tâches, Tâche d'administration, puis Créer une tâche d'administration.
2. Sélectionnez Créer une tâche d'administration et cliquez sur OK.
3. Renseignez l'onglet Profil (page 387).
4. Renseignez l'onglet Rechercher (page 388).
5. Renseignez l'onglet Onglets (page 389).

Remarque : Vous pouvez associer un seul rapport (fichier RPT) à *une seule* tâche de rapport.

Onglet Profil des tâches de rapport

Pour saisir les informations de profil d'une tâche de rapport, cliquez sur l'onglet Profil et renseignez les champs suivants :

Nom

Définit le nom du rapport. Chaque nom de tâche de rapport doit être unique.

Balise

Définit un identificateur unique pour la tâche. Il est utilisé dans une URL, un service Web, ou un fichier de propriétés. Il doit être composé de lettres, de chiffres et/ou de traits de soulignement et commencer par une lettre ou un trait de soulignement.

Catégorie

Spécifie la catégorie à laquelle la tâche actuelle appartient. Sélectionnez la catégorie Génération de rapports pour cette tâche.

Catégorie 2

Spécifie la sous-catégorie à laquelle la tâche actuelle appartient. Saisissez une chaîne dans ce champ.

Objet principal

Spécifie l'objet sur lequel la tâche opèrera. Sélectionnez l'objet principal Instance de rapport.

Action

Spécifie l'action qui sera effectuée avec l'objet principal. Sélectionnez Créer.

Onglet Rechercher des tâches de rapport

La fenêtre de recherche limite la portée de la tâche et contrôle les champs que les utilisateurs peuvent rechercher. Vous pouvez configurer la fenêtre de recherche des rapports en fonction de la transmission dynamique ou non des paramètres aux rapports.

Vous devez créer une fenêtre de recherche distincte pour chaque rapport. La fenêtre de recherche définit les paramètres que vous pouvez utiliser pour filtrer les données de rapport. Lors de la génération d'un rapport, en fonction de la configuration de la fenêtre de recherche, CA IdentityMinder vous invite à saisir les paramètres de filtre des données de rapport. Selon votre saisie, CA IdentityMinder établit une connexion à la base de données de rapports et récupère les données correspondant aux critères.

Pour saisir les informations de recherche d'une tâche de rapport, cliquez sur l'onglet Rechercher et sélectionnez une fenêtre de recherche.

Remarque : Tous les rapports disposent d'une fenêtre de recherche associée. Si vous ne trouvez pas la fenêtre de recherche correspondant à votre rapport, vous devez en créer une. Pour plus d'informations sur la création de fenêtres de recherche de rapports, consultez la rubrique Création d'une fenêtre de recherche de rapports (page 388).

Création d'une nouvelle fenêtre de recherche pour la tâche Rapports

Une fenêtre de recherche de rapports est basée sur la fenêtre par défaut de sélection des types de rapports.

Pour créer une nouvelle fenêtre de recherche pour un rapport :

1. Cliquez sur [...] pour localiser des fenêtres de recherche.

   La liste des fenêtres de recherche disponibles s'affiche.

2. Cliquez sur Nouveau.

   Le volet Création de fenêtre s'affiche.

3. Sélectionnez Fenêtre de sélection des types de rapports dans la liste, puis cliquez sur OK.

   CA IdentityMinder se connecte au serveur de rapports IAM et affiche tous les rapports et leurs critères de recherche en fonction du fichier suitereports.properties.

4. Complétez les champs ci-après.

   Nom

   Définit le nom du rapport. Chaque nom de rapport doit être unique.

   Balise

   Définit un identificateur unique pour la tâche. Il est utilisé pour une URL, un service Web ou des fichiers de propriétés. Il doit être composé de lettres, de chiffres ou caractères de soulignement commençant par une lettre ou un caractère de soulignement.

   Titre

   Définit le titre de la nouvelle fenêtre de recherche. Le titre doit être unique.

   Type de rapport

   Identifie le rapport à associer avec la fenêtre de recherche. Choisissez l'un des rapports que vous avez ajoutés au serveur de rapports IAM.

   La nouvelle fenêtre de recherche est créée pour les rapports.

5. Cliquez sur Ok.

Onglet Onglets des tâches de rapport

Les onglets organisent les champs requis pour l'exécution d'une tâche. Dans un rapport, l'onglet Onglets permet d'associer un rapport à une définition de cliché et de rendre disponible un planificateur de rapports.

Pour configurer l'onglet Onglets d'une tâche de rapport :

1. Cliquez sur Onglets.

   Les onglets visibles pour l'utilisateur s'afficheront.

2. Sélectionnez le contrôleur d'onglets standard.

3. Sélectionnez le planificateur de clichés de rapport à partir duquel les onglets doivent s'afficher dans cette tâche et cliquez sur .

   L'onglet Planificateur de clichés de rapports est ajouté à la liste des onglets.

4. Pour modifier l'onglet Planificateur de clichés de rapports, cliquez sur .

   La fenêtre Configure Report Snapshot Scheduler (Configurer le planificateur de clichés de rapport) s'affiche.

5. Pour associer la tâche de rapport à une définition de cliché, cliquez sur Ajouter.

   Une liste de définitions de clichés (page 355) disponibles s'affichent.

6. Sélectionnez-en une et cliquez sur OK.

   La tâche de rapport est associée à la définition de cliché sélectionnée.

7. Sélectionnez le planificateur de rapports à partir duquel les onglets doivent s'afficher dans cette tâche et cliquez sur .

8. L'onglet Planificateur est ajouté à la liste des onglets.

9. Pour modifier l'onglet Planificateur, cliquez sur .

10. Cliquez sur Soumettre.

    La tâche de rapport est créée.

11. Affectez la tâche de rapport créée à un rôle d'administration.

    L'utilisateur CA IdentityMinder inclus dans le rôle d'administration pourra utiliser cette tâche de rapport tout juste créée.

Rapports par défaut

CA IdentityMinder installe des rapports par défaut, que vous pouvez personnaliser en fonction de vos besoins. Les rapports par défaut sont situés dans le répertoire suivant :

MSSQL

```
<chemin_d'installation>\tools\imrexport\ReportDefinitions\IM Standard
Reports\Ms-SQL Reports
```

Oracle

```
<chemin_d'installation>\tools\imrexport\ReportDefinitions\IM Standard
Reports\Oracle Reports
```

Ces rapports par défaut sont décrits dans le tableau ci-dessous :

Rapport	Définition
Détails du compte	Liste des modèles de comptes et éléments associés : rôles de provisionnement, types de terminaux, terminaux et comptes
administration	Liste des administrateurs et de leurs droits d'administration
Audit - Affectation et retrait des rôles de provisionnement	Liste des événements de rôles de provisionnement
Audit - Déprovisionnement	Liste des comptes d'utilisateurs déprovisionnés
Détails de l'audit	Détails des statuts des tâches et des événements

Rapport	Définition
Audit - Tâches d'approbation en attente	Liste des tâches d'approbation en attente
Mot de passe Audit-Reset	Contient la liste de mots de passe d'utilisateurs réinitialisés au cours d'une période donnée.
Comptes de terminaux	Contient les comptes de terminaux. Vous pouvez sélectionner le terminal à afficher.
Détails du terminal	Liste de tous les types de terminaux, terminaux et attributs de terminaux
Comptes non standard	Contient tous les comptes orphelins, système et d'exception.
Tendances des comptes non standard	Contient les tendances des comptes orphelins, système et d'exception non standard.
Comptes orphelins	Contient tous les comptes de terminal sans utilisateur global dans le serveur de provisionnement.
Stratégies	Contient toutes les stratégies d'identité.
Administrateurs de rôles	Contient les rôles et leurs administrateurs.
Membres avec rôles	Contient les rôles dans la base de données de rapports et répertorie leurs membres.
Propriétaires des rôles	Contient les rôles et leurs propriétaires.
Rôles	Contient les informations suivantes pour chaque rôle de la base de données de rapports : ■ Tâches associées au rôle ■ Stratégies de membre et membres avec rôle ■ Stratégies d'administrateur et administrateurs de rôle ■ Stratégies de propriété et propriétaires de rôle
Clichés	Contient tous les clichés exportés.
Rôles des tâches	Contient les tâches dans la base de données de rapports et les rôles auxquels elles sont associées.
Compte d'utilisateur	Contient une liste d'utilisateurs et leurs comptes. **Remarque :** La liste d'attributs de compte présentée dans ce rapport varie en fonction des attributs exportés.
Droits d'utilisateurs	Contient des rôles, des groupes et des comptes d'utilisateurs. **Remarque :** La liste d'attributs de compte présentée dans ce rapport varie en fonction des attributs exportés.
Statut de synchronisation des stratégies d'utilisateur	Contient le statut d'utilisateur par stratégie (affectation, annulation de l'affectation ou réaffectation de stratégies).

Rapport	Définition
Profil de l'utilisateur	Contient les informations suivantes sur les utilisateurs : ■ Nom ■ ID de l'utilisateur ■ Groupe dont l'utilisateur est membre ou administrateur ■ Rôles dont l'utilisateur est membre, administrateur ou propriétaire
Rôles utilisateur	Contient les rôles affectés à un utilisateur.

Remarque : Pour les rapports de comptes tels que les rapports sur les comptes de terminal et sur les comptes d'utilisateurs, seuls les attributs d'utilisateur par défaut sont exportés.

Le tableau suivant contient une liste d'attributs de compte requis pour les rapports par défaut pour la récupération des données liées aux compte :

Nom du rapport	Attributs requis
Rapport sur les comptes de terminaux	Nom du terminal, date de création, heure de création, date de mise à jour et heure de mise à jour
Rapport non standard	Nom du terminal, date de création, heure de création, date de mise à jour, heure de mise à jour et compte d'exception Sélectionnez la case à cocher Exporter les comptes orphelins.
Rapport sur les tendances des comptes non standard	Nom du terminal, date de création, heure de création, date de mise à jour, heure de mise à jour et compte d'exception Sélectionnez la case à cocher Exporter les comptes orphelins.
Rapport sur les comptes orphelins	Nom du terminal, date de création, heure de création, date de mise à jour, heure de mise à jour et compte d'exception Sélectionnez la case à cocher Exporter les comptes orphelins.
Rapport sur les comptes d'utilisateurs	Nom du terminal, date de création, heure de création, date de mise à jour, heure de mise à jour et compte d'exception Sélectionnez la case à cocher Exporter les comptes orphelins.
Rapport sur les droits des utilisateurs	Nom du terminal, date de création, heure de création, date de mise à jour, heure de mise à jour et compte d'exception Sélectionnez la case à cocher Exporter les comptes orphelins.

Dépannage

La section suivante contient les rubriques de dépannage concernant la génération de rapports.

Redirection vers la page de connexion InfoView lors de l'affichage d'un rapport

Lors de l'affichage d'un rapport dans CA IdentityMinder, il se peut que vous soyez redirigé vers la page de connexion InfoView de BusinessObjects.

Affichage du rapport en cas de redirection

1. Veillez à utiliser un nom de domaine complet pour le serveur de rapports CA (BusinessObjects).
2. Cliquez avec le bouton droit de la souris sur la page Web de connexion InfoView et sélectionnez View Source (Afficher la source).
3. Localisez l'URL du rapport.
4. Copiez-collez cette URL dans une autre fenêtre du navigateur.
5. Si le rapport n'apparaît pas, utilisez un outil de suivi HTTP pour obtenir plus d'informations.
6. Si le rapport apparaît, corrigez les paramètres du navigateur comme suit :
   - Accepter les cookies tiers
   - Autoriser les cookies de session
   - Supprimer les paramètres de niveau de sécurité élevé

Génération de comptes d'utilisateurs pour plus de 20 000 enregistrements

S'il existe plus de 20 000 enregistrements, certaines étapes supplémentaires sont nécessaires pour la génération de rapports de comptes d'utilisateurs.

Pour générer un rapport de comptes d'utilisateurs pour plus de 20 000 enregistrements :

1. Ouvrez la console de gestion centrale BusinessObjects.
2. Cliquez sur Serveurs et sélectionnez *nom_serveur*.pageserver.
3. Sélectionnez Unlimited records (Enregistrements illimités) pour l'entrée Database Records To Read When Previewing Or Refreshing a Report (Lecture des enregistrements de la base de données lors de l'aperçu ou de l'actualisation d'un rapport).
4. Dans Crystal Reports Designer, ouvrez le rapport des comptes d'utilisateurs.
5. Pour définir l'emplacement de votre base de données de clichés, sélectionnez Database (Base de données), puis Set Datasource Location (Définir l'emplacement de la source de données).
6. Enregistrez cette modification.

7. Sous Database (Base de données), Datasource Expert (Expert en sources de données), cliquez avec le bouton droit de la souris sur Command (Commande) dans la fenêtre de droite.

   La syntaxe SQL et la liste des paramètres apparaissent à gauche.

8. Saisissez le nom du paramètre figurant dans les champs des paramètres du modèle de rapport.

9. Modifiez la requête située à gauche et ajoutez le paramètre à cette requête.

   Par exemple, si vous avez sélectionné le paramètre reportid, la requête sera la suivante :

   ```
   Select * from endPointAttributes, endpointview, imreport6
   where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and
   endPointAttributes.imr_reportid = endpointview.imr_reportid
    endpointview.imr_reportid = imreport6.imr_reportid and imreport6.imr_reportid
   = {?reportid}
   ```

10. Enregistrez le rapport.

Chapitre 17: CA User Activity Reporting

Ce chapitre traite des sujets suivants :

Fonctionnalité CA Enterprise Log Manager

Lors de l'intégration de CA Enterprise Log Manager à CA Identity Manager, vous obtenez la fonctionnalité suivante :

- L'agent CA Enterprise Log Manager collecte des informations d'audit de CA Identity Manager et les envoie à CA Enterprise Log Manager pour les convertir en grammaire commune aux événements CA (CEG).
- La console d'utilisateur CA IdentityMinder peut récupérer de manière continue des rapports et/ou des requêtes CA Enterprise Log Manager à l'aide des informations de contexte de CA Identity Manager utilisées pour filtrer les informations renvoyées.
- CA Identity Manager contient de nombreux rapports par défaut, ainsi qu'une infrastructure permettant d'ajouter des rapports et/ou des requêtes CA Enterprise Log Manager à une tâche existante ou nouvelle.
- L'agent CA Enterprise Log Manager est installé dans l'ordinateur CA Identity Manager (base de données d'audit).
- Le connecteur CA Identity Manager est configuré sur l'agent de CA Enterprise Log Manager.
- L'enregistrement du produit CA Enterprise Log Manager pour l'environnement CA Identity Manager est créé.
- Le filtre d'accès aux données de CA Enterprise Log Manager facultatif est créé pour l'enregistrement du produit.

Composants CA Enterprise Log Manager

Lors de l'intégration de CA IdentityMinder à CA Enterprise Log Manager, les composants suivants sont ajoutés à l'architecture CA IdentityMinder :

- Un onglet Visionneuse CA ELM permet d'intégrer des objets CA Enterprise Log Manager dans une tâche nouvelle ou existante.

  Remarque : Vous devez configurer une connexion au serveur CA Enterprise Log Manager.

- Définitions de rôle que vous pouvez importer

Limitations de l'intégration

Vous trouverez ci-après des restrictions connues de l'intégration de la structure au serveur CA Enterprise Log Manager :

- L'exécution de la requête de récupération et des listes de rapports pour la configuration de tâche peut être lente.
- Les API CA Enterprise Log Manager reconnaissent uniquement les fuseaux horaires nommés Java par défaut.
- L'opération Egal à respecte la casse lorsqu'elle est utilisée dans un filtre composé.
- La version minimum du serveur CA Enterprise Log Manager est la version de disponibilité générale (45.10) avec les mises à jour d'abonnement suivantes appliquées par ordre d'apparition :
  1. Patch d'abonnement SP-1
  2. Patch de contenu M5
  3. Mise à jour d'Open API
- Une seule connexion à un serveur CA Enterprise Log Manager à la fois est prise en charge.

Intégration de CA Enterprise Log Manager à CA IdentityMinder

Pour afficher et gérer des rapports et des requêtes CA Enterprise Log Manager, les opérations suivantes doivent être effectuées par un administrateur :

1. Installation de l'agent CA Enterprise Log Manager
2. Création d'un connecteur
3. Activation de l'audit dans CA IdentityMinder
4. Configuration du serveur CA Enterprise Log Manager

Conditions préalables à l'installation de l'agent CA Enterprise Log Manager

Avant d'effectuer l'installation de l'agent CA Enterprise Log Manager, les opérations suivantes doivent être réalisées :

- Veillez à ce que le serveur CA Enterprise Log Manager soit accessible à partir de l'ordinateur exécutant CA IdentityMinder ou hébergeant la base de données d'audit CA IdentityMinder.
- Veillez à ce que l'ordinateur agent soit accessible à partir du serveur.
- Configurez la source de données sur l'ordinateur agent. Pour obtenir des instructions, cliquez ici (page 397).
- Vérifiez que la version d'Adobe Flash Player est la version 9.0.28 ou une version ultérieure. Vous pouvez télécharger Adobe Flash Player à partir du lien suivant :

  http://www.adobe.com/go/getflash
- Téléchargez les fichiers binaires de l'agent. Pour obtenir des instructions, cliquez ici (page 398).
- Obtenez une clé d'authentification pour l'agent. Pour obtenir des instructions, cliquez ici (page 398).
- Facilitez l'accès au nom/à l'IP du serveur.
- Facilitez l'accès aux informations de compte sans compromettre la sécurité. Il s'agit du compte d'identité sous lequel l'agent est exécuté comme service (Windows).
- Si un connecteur existe déjà, exportez les informations par défaut le concernant et facilitez-en l'accès.
- Veillez à ce que l'ordinateur dispose de 4 Go de mémoire RAM.

Configuration de la source de données sur l'ordinateur agent

Pour configurer la source de données sur l'ordinateur agent, suivez la procédure suivante.

Pour configurer la source de données :

1. Accédez au Panneau de configuration, Outils d'administration, Sources de données (ODBC).
2. Dans l'onglet Nom DSN système, ajoutez l'élément suivant :

   Source de données imsauditevent12 (ODBC) pointant vers la base de données d'audit
3. Cliquez sur Appliquer/OK.

   La source de données est configurée.

Téléchargement des fichiers binaires de l'agent

Pour télécharger des fichiers binaires de l'agent, suivez la procédure suivante.

Pour télécharger les fichiers binaires de l'agent

1. Connectez-vous au serveur CA Enterprise Log Manager à l'aide de l'URL suivante :

   https://<hôte>:5250/spin/calm/CALMSpindle.csp

2. Accédez à Administration, Collecte de journaux, Explorateur d'agent, Télécharger des fichiers binaires d'agent, <SE> <version>.

3. Enregistrez sous Fichier.

Obtention d'une clé d'authentification pour l'agent

Pour obtenir la clé d'authentification d'agent, suivez la procédure suivante.

Pour obtenir la clé d'authentification de l'agent

1. Dans le serveur CA Enterprise Log Manager, accédez à Administration, Collecte de journaux, Explorateur d'agent, Clé d'authentification d'agent.

2. Facilitez l'accès à la clé sans compromettre la sécurité.

Installation de l'agent CA Enterprise Log Manager

L'agent CA Enterprise Log Manager est responsable de la collecte d'événements et de l'envoi de ces informations au serveur CA Enterprise Log Manager. Pour activer la journalisation, installez l'agent sur un serveur de base de données ou un terminal CA IdentityMinder.

Remarque : L'agent CA Enterprise Log Manager est pris en charge sous Windows et Linux.

Pour installer l'agent CA Enterprise Log Manager :

1. Sur le serveur de base de données, exécutez l'installation du fichier ca-elmagent-<version>.exe et spécifiez l'élément suivant :

   Nom/IP adresse du serveur CA Enterprise Log Manager et code d'authentification

   Informations sur le compte de serveur de l'agent à utiliser pour exécuter l'agent comme service/démon
2. Le cas échéant, spécifiez le fichier de liste de connecteurs par défaut.
3. Connectez-vous au serveur CA Enterprise Log Manager à l'aide de l'URL suivante :

   https://<hôte> :5250/spin/calm/CALMSpindle.csp
4. Accédez à Administration, Collecte de journaux, Explorateur d'agent, Groupe d'agents par défaut.
5. Sélectionnez l'ordinateur agent et lancez la vue Statut et commande.

   Le statut doit être en cours d'exécution.

Importation de définitions de rôles

Pour configurer la connexion à CA Enterprise Log Manager dans la console d'utilisateur, vous devez d'abord importer des définitions de rôles CA Enterprise.

Pour importer des définitions de rôles :

1. Connectez-vous à la console de gestion à l'aide de l'URL suivante.

   `http://`*`hôte`*`:`*`port`*`/iam/immanage`
2. Accédez à Environnement, Role and Task Settings (Paramètres de rôles et de tâches), cliquez sur Importer et sélectionnez le fichier Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml.
3. Cliquez sur Enregistrer et fermer.
4. Dans l'onglet Système de la console d'utilisateur, cliquez sur Configurer la connexion CA Enterprise Log Manager, renseignez les informations requises et cliquez sur Soumettre.

Création d'un connecteur

Pour créer un connecteur, suivez la procédure suivante.

Pour créer un connecteur :

1. Connectez-vous au serveur CA Enterprise Log Manager à l'aide de l'URL suivante :

   `https://<hôte> :5250/spin/calm/CALMSpindle.csp`

2. Accédez à Administration, Collecte de journaux, Explorateur d'agent, Groupe d'agents par défaut.

3. Sélectionnez l'ordinateur agent.

4. Basculez vers la vue Connecteurs.

5. Cliquez sur Créer un connecteur et saisissez les informations suivantes :

   Détails du connecteur

   Sélectionnez le type d'intégration CAIdentityManager et modifiez le nom du connecteur si vous le souhaitez.

   Configuration des connecteurs

   Chaîne de connexion

   - Driver={SQL Server} ; Server=<Auditing DB Server> ; Database=<Auditing DB>
   - Driver={Microsoft ODBC for Oracle} ; Dbq=<Auditing DB TNSname>

   Nom d'utilisateur : <Utilisateur de la BdD d'audit>

   Mot de passe : <Mot de passe de l'utilisateur de la BdD d'audit>

6. Appliquez les changements de configuration de la connexion suivants au connecteur CA Identity Manager à utiliser avec r12.6.1.

   - SourceName (Nom de la source) : il s'agit du nom de la source de données sur l'ordinateur de l'agent (imsauditevent12).
   - AnchorSQL (Ancrage SQL) : sélectionnez max(id) dans imsauditevent12.
   - AnchorField (Champ d'ancrage) : IMS_EVENTID
   - Evénement SQL :

```
select imsauditevent12.id as IMS_EVENTid ,imsauditevent12.audit_time as
IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME
,imsauditevent12.admin_name as ADMINUNIQUENAME ,imsauditevent12.admin_dn as
ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID
,imsauditevent12.event_description as EVENTINFO
,imsauditevent12.event_state as EVENTSTATE
,imsauditevent12.tasksession_oid as TASKOID
,imsaudittasksession12.task_name as TASKNAME
,imsauditeventobject12.object_type as OBJECTTYPE ,
imsauditeventobject12.object_name as
```

```
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as ATTRNAME
,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRNEWVALUE
,imsauditobjectattributes12.attribute_newvalue as ATTRVALUE from
imsaudittasksession12, imsauditevent12, imsauditeventobject12,
imsauditobjectattributes12 where imsauditevent12.id >? and
imsauditevent12.tasksession_id = imsaudittasksession12.id and
imsauditevent12.tasksession_oid = imsaudittasksession12.tasksession_oid
and
imsauditeventobject12.parent_event_id = imsauditevent12.id and
imsauditobjectattributes12.parent_object_id = imsauditeventobject12.id
ORDER BY
imsauditevent12.id ASC;
```

7. Enregistrez et fermez.

Pour vérifier le fonctionnement du connecteur :

1. Accédez à Administration, Collecte de journaux, Explorateur d'agent, Groupe d'agents par défaut.
2. Sélectionnez l'ordinateur agent.
3. Basculez vers la vue Connectors (Connecteurs) et cliquez sur le bouton Launch Status and Command View (Lancer la vue Statut et commande).

   Le statut doit être en cours d'exécution.

Activation de l'audit dans CA Identity Manager

Pour activer l'audit dans CA Identity Manager :

1. Ouverture de la console de gestion

   `http://hôte:port//iam/immanage`

2. Accédez à Environnements, <Environnement>, Paramètres avancés, Audit.
3. Exportez les paramètres existants et enregistrez le fichier.
4. Ajoutez les éléments suivants au fichier enregistré et enregistrez les modifications :
   - <Audit enabled="true" auditlevel="BOTH" datasource="auditDbDataSource"
   - Sous le dernier profil d'audit déjà défini, ajoutez le profil d'audit des stratégies de mots de passe :

     <AuditProfile objecttype="FWPASSWORDPOLICY" auditlevel="BOTHCHANGED"/>
5. Pour déclencher le cumul d'informations d'audit, réimportez le fichier dans la console de gestion et effectuez l'une des opérations suivantes :
   - Tâches effectuées sur l'objet géré Utilisateur
   - Tâches effectuées sur l'objet géré Groupe
   - Tâches effectuées sur l'objet géré Stratégies de mots de passe
6. Connectez-vous au serveur CA Enterprise Log Manager à l'aide de l'URL suivante :

   https://<hôte> : 5250/spin/calm/CALMSpindle.csp
7. Pour exécuter des rapports existants, accédez à Requêtes et rapports, Requêtes, CA Identity Manager.

   Remarque : Le serveur CA Enterprise Log Manager doit déjà être configuré.
8. En fonction des tâches effectuées, ouvrez les rapports par défaut suivants et vérifiez l'entrée des événements :
   - La tâche Tous les événements du système par utilisateur appelle CA Identity Manager - Tous les événements du système filtrés par ID d'utilisateur.
   - La tâche Gestion des comptes par hôte appelle la gestion des comptes par hôte telle quelle.
   - La tâche Créations de comptes par compte appelle les créations de comptes par compte telles quelles.
   - La tâche Suppressions de compte par compte appelle les suppressions de compte par compte telles quelles.
   - La tâche Verrouillages de comptes par compte appelle les verrouillages de comptes par compte telles quelles.
   - La tâche Activité de processus de certification par hôte appelle CA Identity Manager - Activité de processus par hôte telle quelle.

- La tâche Activité de modification de stratégie de mot de passe appelle CA Identity Manager - Activité de modification de stratégie telle quelle.

Configuration du serveur CA Enterprise Log Manager

Pour configurer le serveur CA Enterprise Log Manager à gérer, vérifiez les points suivants :

- Vous devez disposer des informations d'identification de l'administrateur Eiam.
- Vous devez disposer de la version 9.0.28 d'Adobe Flash Player ou d'une version ultérieure.

Suite à la configuration du serveur CA Enterprise Log Manager, la fonctionnalité suivante est disponible :

- Plusieurs environnements produisant des événements d'audit sont consommés par un serveur CA Enterprise Log Manager unique ou par une hiérarchie fédérée.
- Vous pouvez implémenter l'autorisation d'accès aux données de systèmes distants via le filtre d'accès aux données CA Enterprise Log Manager.

Pour configurer le serveur CA Enterprise Log Manager :

1. A l'aide de l'URL suivante, connectez-vous à la page d'enregistrement de produit du serveur CA Enterprise Log Manager avec les informations d'identification de l'administrateur de CA Enterprise Log Manager :

   ```
   https://host:port/spin/calmapi/products.csp
   ```

2. Pour enregistrer votre environnement CA IdentityMinder, cliquez sur Enregistrer et indiquez le nom et le mot de passe de votre certificat.

   Remarque : Chaque environnement doit disposer de paires d'enregistrement distinctes (nom/mot de passe de certificat).

3. Accédez à Administration, User and Access Management (Gestion des utilisateurs et des accès), New Data Access Filter (Nouveau filtre d'accès) et indiquez un nom pour la création du filtre.
4. Passez à l'étape suivante.
5. Laissez l'option Identités sélectionnées définie sur Toutes les identités et passez à l'étape suivante.
6. Pour créer un filtre d'accès, cliquez sur Nouveau filtre d'événement.

   Pour configurer le filtre d'accès aux données, limitez le certificat créé au nom d'ordinateur/environnement uniquement pour les journaux collectés à partir de CA IdentityMinder. Vous pouvez également limiter le certificat de sorte à accéder uniquement aux informations natives des terminaux gérés.

7. Enregistrez et fermez.
8. Pour ouvrir les stratégies d'accès, cliquez sur Open Access Policies (Ouvrir les stratégies d'accès).
9. Sélectionnez Obligation Policies (Stratégies d'obligation) et cliquez sur la seule stratégie disponible.

10. Supprimez le texte Toutes les identités et ajoutez le nom du certificat.
11. Enregistrez la stratégie.
12. Connectez-vous à la console d'utilisateur CA Identity Manager et configurez la connexion à CA Enterprise Log Manager.

Configuration de la connexion CA Enterprise Log Manager

La fenêtre Configurer la connexion CA Enterprise Log Manager permet de gérer les tâches de connexion ajoutées à CA Enterprise Log Manager.

Les champs qu'elle contient sont répertoriés ci-dessous.

Nom de la connexion

Spécifie le nom unique utilisé pour l'objet géré de connexion CA ELM unique.

Il s'agit d'un champ en lecture seule.

Description

Décrit la connexion CA ELM.

Nom d'hôte

Spécifie le nom d'hôte et l'adresse IP du serveur CA Enterprise Log Manager.

Ce champ est obligatoire.

Nº de port

Spécifie le port de connexion du serveur CA Enterprise Log Manager.

Valeur par défaut : 52 520

Ce champ est obligatoire.

Certificat SSL signé par une autorité de certification

Lorsque cette option est activée, elle spécifie une vérification de certificat stricte lors de la connexion à un serveur CA Enterprise Log Manager.

Si vous disposez d'un certificat SSL auto-signé, installé par exemple avec CA Enterprise Log Manager par défaut, cette case à cocher ne doit pas être activée car le chemin approuvé vers l'autorité de certification racine n'existe pas.

Nom du certificat

Spécifie le nom du certificat CA Enterprise Log Manager à utiliser pour l'authentification.

Ce champ est obligatoire.

Mot de passe du certificat

Spécifie le mot de passe du serveur CA Enterprise Log Manager.

Ce champ est obligatoire.

Attribut

Non pris en charge. La version est récupérée lors d'une tentative d'enregistrement des informations de connexion comme test.

Suppression de la connexion Enterprise Log Manager

Sélectionnez une connexion dans la liste, puis cliquez sur Supprimer. La tâche de connexion CA Enterprise Log Manager est supprimée.

Intégration de rapports ou requêtes CA Enterprise Log Manager supplémentaires à CA Identity Manager

Vous pouvez intégrer des rapports ou des requêtes CA Enterprise Log Manager supplémentaires à CA Identity Manager à l'aide de l'onglet Visionneuse CA Enterprise Log Manager. Vous pouvez combiner ces nouveaux rapports ou requêtes avec des tâches existantes (y compris des assistants) ou nouvelles. Des données fédérées CA Enterprise Log Manager peuvent également être incluses si vous le souhaitez. A l'aide de l'onglet Visionneuse CA Enterprise Log Manager, vous pouvez appliquer des filtres aux informations récupérées. Ces filtres peuvent utiliser les éléments suivants :

- Valeurs constantes
- Attributs d'objet géré
  - Par exemple, physiques - ::MyPhysicalAttribute::

    logiques - ::|MyLogicalAttribute|::
- Tout champ tel que décrit par la grammaire commune aux événements de CA Enterprise Log Manager (CEG)
  - dest_username
  - dest_objectname
  - dest_uid
  - source_username
  - source_objectname
  - source_uid
  - ...

Configuration de l'onglet Visionneuse CA Enterprise Log Manager

Configurez l'onglet Visionneuse CA Enterprise Log Manager pour s'afficher avec tout ou partie des champs suivants.

Nom

Nom que vous affectez à l'onglet.

Balise

Identifiant unique pour l'onglet au sein de la tâche. Elle doit commencer par une lettre ou un caractère de soulignement et contenir uniquement des lettres, des chiffres ou des caractères de soulignement. La balise est principalement utilisée pour définir des valeurs de données via des documents XML ou des paramètres HTTP.

Masquer l'onglet

Empêche l'onglet d'être visible dans la tâche. Cette option est utile pour les applications qui doivent masquer l'onglet, mais qui ont toujours accès aux attributs de cet onglet.

Requête CA Enterprise Log Manager

Spécifie que les requêtes CA Enterprise Log Manager sont affichées.

Remarque : Vous devez spécifier soit Requête CA Enterprise Log Manager, soit Rapport CA Enterprise Log Manager.

Rapport CA Enterprise Log Manager

Spécifie que les rapports CA Enterprise Log Manager sont affichés.

Remarque : Vous devez spécifier soit Requête CA Enterprise Log Manager, soit Rapport CA Enterprise Log Manager.

ID CA Enterprise Log Manager

Spécifie l'ID de la requête ou du rapport.

Inclure les données fédérées

Inclut ou exclut les données fédérées CA Enterprise Log Manager dans les résultats. Par défaut, ce champ est activé.

Afficher l'invite

Spécifie les requêtes d'invite CA Enterprise Log Manager uniquement. Par défaut, ce champ est activé.

Filtre

Spécifie les conditions avancée SQL permettant d'affiner les résultats renvoyés par les requêtes ou les rapports CA Enterprise Log Manager. Vous pouvez inclure des valeurs constantes et dynamiques. Voici un exemple d'expression.

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username EQUAL
::logical.attribute.Y:: ))
```

Les opérations prises en charge sont les suivantes.

- égal(e) à (EQUAL)
- différent(e) de (NEQ)
- inférieur(e) à (LESS)
- supérieur(e) à (GREATER)
- inférieur(e) ou égal(e) à (LEQ)
- supérieur(e) ou égal(e) à (GREATEQ)
- comme (LIKE)
- distinct de (NOTLIKE)
- dans l'ensemble (INSET)
- extérieure à l'ensemble (NOTINSET)

Les conjonctions utilisées sont les suivantes.

- ET
- OU

Les parenthèses sont obligatoires. Si la valeur à gauche de l'expression de condition n'a pas le marqueur "::" aux deux extrémités, elle est considérée comme une constante et envoyée à CA Enterprise Log Manager telle quelle.

Tableau Paramètre/Valeur

Spécifie les champs et les valeurs à utiliser pour la portée.

Seuls les requêtes et rapports correspondants aux balises et à la logique de balises de portée sont sélectionnés.

Paramètre

Spécifie les valeurs des paramètres Démarrer, Arrêter et Limite. Les paramètres suivants sont pris en charge.

- Granularité horaire (pour les tendances uniquement)
- Heure de début
- Heure de fin
- Date postérieure au premier événement groupé (pour les requêtes groupées uniquement)
- Date postérieure au dernier événement groupé (pour les requêtes groupées uniquement)
- Date antérieure au dernier événement groupé (pour les requêtes groupées uniquement)
- Nombre minimum d'événements de regroupement (pour les requêtes groupées uniquement)

- Nombre maximum d'événements de regroupement (pour les requêtes groupées uniquement)

Chapitre 18: Flux de travaux

Ce chapitre traite des sujets suivants :

Présentation d'un flux de travaux

La fonctionnalité de flux de travaux d'CA IdentityMinder permet à une tâche d'CA IdentityMinder d'être contrôlée par un processus de flux de travaux. Un *processus de flux de travaux* se compose d'une ou plusieurs étapes qui doivent être effectuées avant que CA IdentityMinder puisse terminer une tâche sous le contrôle d'un flux de travaux. Un *job* est une instance d'exécution d'un processus de flux de travaux.

WorkPoint Designer est un logiciel de la société Workpoint LLC, filiale de Planet Group, Inc., intégré à CA IdentityMinder. WorkPoint Designer vous permet de gérer des processus de flux de travaux et des jobs de flux de travaux.

Un processus de flux de travaux consiste en une ou plusieurs étapes, appelées *activités*, qui doivent être effectuées afin d'accomplir une tâche commerciale, comme créer ou modifier le compte d'utilisateur d'un employé. En général, le processus de flux de travaux inclut une ou plusieurs activités manuelles qui nécessitent un utilisateur autorisé ou un participant pour approuver ou rejeter la tâche.

Un *participant* est une personne qui est autorisée à effectuer une activité de flux de travaux. Dans CA IdentityMinder, les participants sont aussi appelés *approbateurs*, étant donné qu'ils doivent approuver ou rejeter la tâche sous le contrôle d'un flux de travaux. Un *outil de résolution de participants* est une règle ou un ensemble de critères pour déterminer qui sont les participants.

Les activités manuelles individuelles d'un flux de travaux sont appelées *tâches* dans CA IdentityMinder.

Une *liste de travail* est une liste de tâches d'approbation ou *de tâches* générée par le flux de travaux, qui apparaît dans la console d'utilisateur du participant autorisé à approuver la tâche.

Diagramme de processus de flux de travaux

Les tâches CA IdentityMinder déclenchent généralement des événements CA IdentityMinder. Par exemple, pour créer un utilisateur, un administrateur sélectionne une tâche Créer un utilisateur. Lorsque cette tâche est commencée, l'événement CreateUserEvent est déclenché.

Le diagramme suivant est un exemple d'un processus de flux de travaux simple (le processus prédéfini CreateUserApproveProcess), tel qu'il apparaît dans WorkPoint Designer. Ce processus est appelé par un CreateUserEvent si la tâche Créer un utilisateur est sous le contrôle d'un flux de travaux.

Le processus inclut l'activité manuelle Approuver la création d'un utilisateur qui correspond à une tâche d'approbation de flux de travaux CA IdentityMinder portant le même nom. Le participant doit approuver ou rejeter la tâche d'approbation, généralement en cliquant sur un bouton dans la console d'utilisateur, avant que la tâche sous le contrôle d'un flux de travaux soit achevée.

Flux de travaux et courriel de notification

Lorsque vous lancez une tâche, CA IdentityMinder la soumet pour traitement et affiche le message d'accusé de réception ci-après.

```
Confirmation : La tâche est terminée.
```

Toutefois, si la tâche est sous le contrôle d'un flux de travaux et nécessite une approbation, le message suivant s'affiche.

```
Alerte : La tâche est en attente.
```

Outre les messages qui s'affichent à l'écran, CA IdentityMinder peut générer automatiquement des courriels de notification dans les cas suivants.

- Un événement ou une tâche nécessitant une approbation ou un rejet par un approbateur de flux de travaux est en attente.
- Un approbateur approuve un événement ou une tâche.

- Un approbateur rejette un événement ou une tâche.
- Un événement ou une tâche est terminée.

Informations complémentaires :

Notifications par courriel (page 515)

Documentation de WorkPoint

Pour obtenir des informations générales sur les concepts de flux de travaux et des instructions sur les processus de flux de travaux, les activités et les jobs dans WorkPoint Designer, reportez-vous à la documentation de WorkPoint. Pour ce faire, ouvrez la page HTML suivante :

`outils_admin\WorkPoint\docs\designer\default.htm`

outils_admin

Définit le répertoire d'installation des outils administration CA IdentityMinder. Le chemin d'installation par défaut est le suivant.

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_d'installation2>/tools

Remarque : Workpoint est un produit tiers installé avec CA IdentityMinder. CA IdentityMinder prend en charge un sous-ensemble de fonctionnalités dans WorkPoint. Par exemple, CA IdentityMinder ne prend pas en charge la console WpConsole. Toutefois, la documentation de WorkPoint décrit toutes les fonctionnalités du produit. Des parties de la documentation de Workpoint ne s'appliquent pas aux utilisateurs de CA IdentityMinder.

Méthodes de contrôle du flux de travaux

CA IdentityMinder propose deux méthodes permettant de placer des tâches sous le contrôle d'un flux de travaux.

Méthodes des modèles

CA IdentityMinder inclut des modèles de processus de flux de travaux que vous pouvez utiliser pour placer des tâches sous le contrôle d'un flux de travaux. La *méthode des modèles* vous permet d'utiliser ces modèles pour configurer et gérer entièrement le flux de travaux à partir de la console d'utilisateur. Introduits dans la version r12 d'CA IdentityMinder, ces modèles de processus génériques peuvent être configurés pour contrôler la plupart des tâches et des événements CA IdentityMinder.

La méthode des modèles active les nouvelles fonctionnalités ci-dessous.

- un contrôle du flux de travaux au niveau tâche et au niveau événement ;
- une configuration simplifiée de l'outil de résolution de participants pour les approbateurs de flux de travaux ;
- Une délégation des tâches, qui couvre des scénarios d'absence du bureau en autorisant un utilisateur à déléguer l'approbation des tâches à un autre utilisateur.
- Une réaffectation des tâches, qui permet de réaffecter une tâche en cours d'exécution à un autre utilisateur pour approbation.

Méthode WorkPoint

CA IdentityMinder inclut également un ensemble de processus de flux de travaux prédéfinis avec des mappages d'événements par défaut qui correspondent à des tâches spécifiques CA IdentityMinder. La *méthode WorkPoint* nécessite que vous configuriez et personnalisiez ces processus à partir de WorkPoint Designer. Ces processus prédéfinis sont compatibles avec des versions antérieures à la version r12 d'CA IdentityMinder.

La méthode Workpoint active également les nouvelles fonctionnalités ci-dessous.

- un contrôle du flux de travaux au niveau tâche et au niveau événement ;
- Une délégation des tâches, qui couvre des scénarios d'absence du bureau en autorisant un utilisateur à déléguer l'approbation des tâches à un autre utilisateur.
- Une réaffectation des tâches, qui permet de réaffecter une tâche en cours d'exécution à un autre utilisateur pour approbation.

Remarque : Pour une meilleure souplesse et commodité, CA vous recommande d'utiliser la méthode des modèles dans la mesure du possible.

Informations complémentaires :

Méthodes des modèles (page 420)
Méthode WorkPoint (page 442)

Activation du flux de travaux

Vous devez activer le flux de travaux avant de pouvoir l'utiliser pour contrôler les tâches CA IdentityMinder. Par défaut, le flux de travaux est désactivé.

Pour activer le flux de travaux

1. Dans la console de gestion, sélectionnez un environnement.
2. Accédez à Paramètres avancés, Flux de travaux.
3. Activez la case à cocher Activé, puis cliquez sur Enregistrer.

   Remarque : Les mappages des événements sur cette fenêtre s'appliquent uniquement si vous utilisez la méthode WorkPoint pour configurer le flux de travaux. Si vous utilisez la méthode des modèles (recommandée), ne mappez pas des événements aux processus à l'aide de cette console de gestion.

4. Redémarrez le serveur d'applications.
5. (Facultatif) Configurez les outils d'administration WorkPoint (page 415).

Informations complémentaires :

Méthodes de contrôle du flux de travaux (page 413)
Mapper un processus vers un événement globalement (page 446)

Configuration des outils d'administration WorkPoint

WorkPoint Designer est un logiciel de la société Workpoint LLC, filiale de Planet Group, Inc., intégré à CA IdentityMinder. WorkPoint Designer vous permet de gérer des processus de flux de travaux et des jobs de flux de travaux. Les outils d'administration WorkPoint incluent WorkPoint Designer et WorkPoint Archive. Afin de configurer les outils d'administration WorkPoint Administrative Tools, installez les outils d'administration CA IdentityMinder. Pour ce faire, exécutez le programme d'installation et sélectionnez l'option Outils d'administration CA IdentityMinder.

Remarque : Pour utiliser les outils d'administration pour le flux de travaux, un JDK pris en charge doit être installé sur le système sur lequel les outils d'administration résident. Pour obtenir une liste exhaustive des versions et des plates-formes prises en charge, consultez le site de support technique de CA IdentityMinder.

Les outils clients de flux de travaux sont situés dans le répertoire WorkPoint des outils d'administration d'CA IdentityMinder. Les outils d'administration sont installés aux emplacements par défaut ci-après.

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_d'installation2>/tools

Les outils figurant dans ce répertoire vous permettent d'effectuer les opérations suivantes.

- Création du schéma de base de données de flux de travaux
- Chargement des scripts de flux de travaux par défaut
- Conception et suivi des processus et jobs de flux de travaux

Configuration des outils d'administration WorkPoint sous JBoss

Pour configurer les outils d'administration WorkPoint sous JBoss, modifiez les fichiers init.bat/sh et workpoint-client.properties.

Modification du fichier init.bat/init.sh

Pour modifier le fichier init.bat/init.sh :

1. Dans un éditeur de texte, modifiez l'un des fichiers ci-dessous.
   - **Windows :**

     outils_admin\Workpoint\bin\init.bat
   - **UNIX :**

     *outils_admin/*Workpoint/bin/init.sh
2. Supprimez les commentaires de la ligne EJB_CLASSPATH dans la section JBoss du fichier.

   Remarque : Vérifiez que toutes les sections des autres serveurs d'applications sont commentées.
3. Copiez jbossall-client.jar de *accueil_jboss*\client\ vers :

   outils_admin\Workpoint\lib

Modification du fichier workpoint-client.properties

Modifiez le fichier workpoint-client.properties en fonction du type de serveur d'applications sélectionné au cours de l'installation de CA IdentityMinder.

Pour configurer le fichier workpoint-client.properties :

1. Ouvrez *outils_admin*\Workpoint\conf\
   workpoint-client.properties dans un éditeur de texte.

   outils_admin est l'emplacement d'installation des outils d'administration. Les outils d'administration sont installés aux emplacements par défaut ci-après.

   - **Windows :** <chemin_d'installation>\tools
   - **UNIX :** <chemin_d'installation2>/tools

2. Localisez la section intitulée JBOSS SETTINGS.

3. Supprimez les valeurs de propriétés de cette section.

   comme les exemples ci-dessous.

   ```
   java.naming.provider.url=localhost
   java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
   java.naming.factory.url.pkgs=org.jboss.naming
   ```

   Remarque : Il se peut que vous deviez modifier la valeur de la propriété java.naming.provider.url. Par exemple, remplacez localhost par jnp://*nom_ou_adresse_ip_ du serveur*:*port*. Utilisez le numéro de port 1099.

4. Enregistrez le fichier.

Configuration des outils d'administration WorkPoint sous WebLogic

Pour configurer les outils d'administration WorkPoint sous WebLogic, modifiez les fichiers init.bat/sh et workpoint-client.properties.

Modification du fichier init.bat/init.sh

Pour modifier le fichier init.bat/init.sh :

1. Dans un éditeur de texte, modifiez l'un des fichiers ci-dessous.
   - **Windows :**

     outils_admin\Workpoint\bin\init.bat
   - **UNIX :**

     outils_admin/Workpoint/bin/init.sh
2. Supprimez les commentaires de la ligne EJB_CLASSPATH dans la section WebLogic du fichier.

   Remarque : Vérifiez que toutes les sections des autres serveurs d'applications sont commentées.
3. Copiez le fichier wlclient.jar de *accueil_weblogic*\server\lib vers l'emplacement suivant.

   outils_admin\Workpoint\lib\

Modification du fichier workpoint-client.properties

Modifiez le fichier workpoint-client.properties en fonction du type de serveur d'applications sélectionné au cours de l'installation de CA IdentityMinder.

Pour configurer le fichier workpoint-client.properties :

1. Ouvrez *outils_admin*\Workpoint\conf\ workpoint-client.properties dans un éditeur de texte.
2. Localisez la section WebLogic du fichier.
3. Supprimez les commentaires sur toutes les valeurs de propriétés de cette section.
4. Enregistrez le fichier.

   Remarque : La propriété java.naming.provider.url doit pointer vers le nom de domaine complet et le numéro de port WebLogic du système sur lequel le serveur CA IdentityMinder est installé.

Configuration des outils d'administration WorkPoint sous WebSphere

Pour configurer les outils d'administration WorkPoint sous WebSphere, modifiez les fichiers init.bat/sh et workpoint-client.properties.

Modification du fichier init.bat/init.sh

Pour modifier le fichier init.bat/init.sh :

1. Dans un éditeur de texte, modifiez l'un des fichiers ci-dessous.
   - **Windows :**

     outils_admin\Workpoint\bin\init.bat
   - **UNIX :**

     outils_admin/Workpoint/bin/init.sh
2. Supprimez les commentaires de la section IBM WebSphere.

   Remarque : Ne commentez pas l'entrée WP_CLASSPATH de la section COMMON WP_CLASSPATH.
3. Vérifiez que toutes les sections des autres serveurs d'applications sont commentées.
4. Remplacez les valeurs pour JAVA_HOME et WAS_HOME par les chemins appropriés pour votre environnement.

Modification du fichier workpoint-client.properties

Modifiez le fichier workpoint-client.properties en fonction du type de serveur d'applications sélectionné au cours de l'installation de CA IdentityMinder.

Pour configurer le fichier workpoint-client.properties :

1. Ouvrez *outils_admin*\Workpoint\conf\ workpoint-client.properties dans un éditeur de texte.

   outils_admin est l'emplacement d'installation des outils d'administration. Les outils d'administration sont situés aux emplacements par défaut ci-après.
   - **Windows :** <chemin_d'installation>\tools
   - **UNIX :** <chemin_d'installation2>/tools
2. Localisez la section intitulée IBM WEBSPHERE SETTINGS.
3. Supprimez les valeurs de propriétés de cette section.

   Exemple :
   ```
   java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFactory
   java.naming.provider.url=iiop://localhost:bootstrap_port
   ```
   Remarque : Le numéro de port d'amorçage doit correspondre au numéro de port spécifié dans la console d'administration WebSphere. Pour localiser le numéro de port, accédez à Serveur, Terminaux, Adresse du serveur d'amorçage.

4. Mettez à jour le port BOOTSTRAP_ADDRESS pour le profil WebSphere comme suit.
   a. Dans la console d'administration WebSphere, accédez à Serveurs d'applications, nom_du_serveur, Communications.
   b. Développez les ports.
   c. Modifiez le fichier workpoint-client.properties situé sous iam_im.ear/config.
   d. Remplacez le port par défaut 2809 dans la section WebSphere par le port du profil pour BOOTSTRAP_ADDRESS.
5. Enregistrez le fichier.

Lancement de WorkPoint Designer

Pour lancer WorkPoint Designer, exécutez le fichier suivant :

- **Windows :** *outils_admin*\WorkPoint\bin\Designer.bat
- **UNIX :** *outils_admin*/WorkPoint/bin/Designer.sh

où *outils_admin* est le répertoire d'installation des outils d'administration d'CA IdentityMinder. Les outils d'administration sont installés aux emplacements par défaut ci-après.

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_d'installation2>/tools

Remarque : Les composants du flux de travaux installés doivent être configurés pour que vous puissiez exécuter WorkPoint Designer. Pour obtenir des instructions, consultez la section "Configuration des outils d'administration WorkPoint" de votre serveur d'applications.

Informations complémentaires :

Configuration des outils d'administration WorkPoint sous JBoss (page 416)
Configuration des outils d'administration WorkPoint sous WebLogic (page 417)
Configuration des outils d'administration WorkPoint sous WebSphere (page 418)

Méthodes des modèles

Introduite dans la version r12 d'CA IdentityMinder, la méthode des modèles vous permet de configurer les modèles de processus de flux de travaux dans la console d'utilisateur sans ouvrir WorkPoint Designer.

Les avantages de la méthodes des modèles sont les suivants :

- des modèles de processus échelonnés peuvent répondre à la plupart des besoins d'un flux de travaux sans nécessiter de personnalisation dans WorkPoint Designer ;
- les modèles prennent en charge les flux de travaux au niveau tâche et au niveau événement ;
- le même modèle de processus de flux de travaux peut être configuré pour être utilisé avec de nombreuses tâches, tandis que la conception du processus lui-même reste la même ;
- il est facile de spécifier les outils de résolution de participants dans la console d'utilisateur ;
- La délégation des tâches peut s'effectuer dans la console d'utilisateur.

Modèles de processus

Un modèle de processus de flux de travaux a les caractéristiques suivantes.

- Il est défini dans WorkPoint Designer.
- Il est constitué d'activités manuelles, qui correspondent aux tâches d'approbation CA IdentityMinder.
- Il inclut des attributs spéciaux contenant des informations pour identifier les participants (également appelés approbateurs).

Les modèles de processus de flux de travaux ne comprennent aucune information permettant de sélectionner des participants précis. C'est CA IdentityMinder qui permet de le faire une fois que l'utilisateur a configuré un flux de travaux et son outil de résolution de participants. Ces informations sont mappées vers un événement pour un contrôle de flux de travaux au niveau événement et vers une tâche pour un contrôle de flux de travaux au niveau tâche.

Lorsque vous utilisez la méthode des modèles, la configuration des flux de travaux et des participants s'effectue dans la console d'utilisateur.

Il existe trois modèles de processus à utiliser dans le cadre de la méthode des modèles :

- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

Fonctionnement d'un modèle de processus

Un modèle de processus de flux de travaux contient un certain nombre d'emplacements où une liste des participants est requise. Lorsque le modèle est mappé vers une tâche ou un événement CA IdentityMinder, vous devez configurer l'outil de résolution de participants pour ces listes.

Pendant l'exécution, comme indiqué dans la capture ci-après, CA IdentityMinder fournit la liste des participants au processus de flux de travaux en fonction de vos informations de configuration.

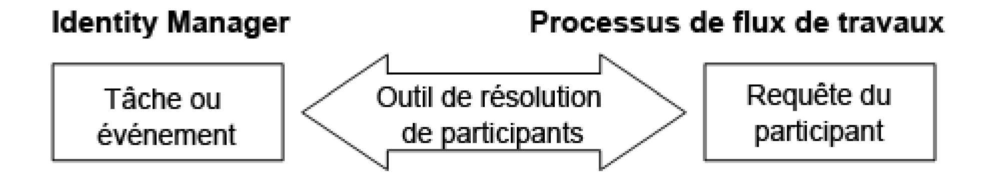


Diagramme de modèle en une seule étape

Le diagramme suivant illustre le modèle de processus SingleStageApproval tel qu'il apparaît dans WorkPoint Designer. Le modèle de processus inclut deux activités manuelles :

- un noeud d'approbation pour le participant principal. Si cet utilisateur approuve ou rejette la requête, le processus s'exécute entièrement ;
- un noeud d'approbation pour le participant par défaut. Cet utilisateur peut approuver ou rejeter la tâche si le participant principal n'est pas trouvé ou ne répond pas.

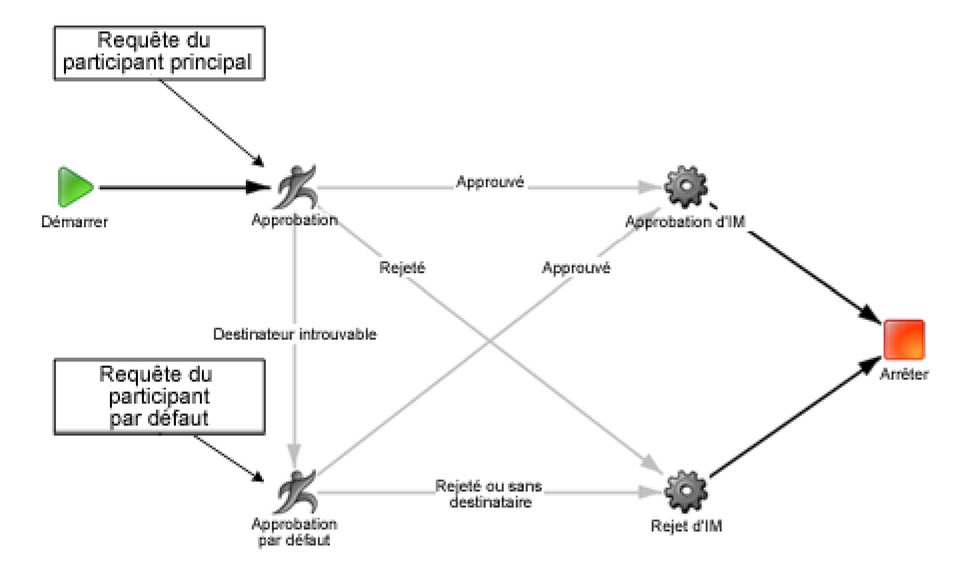


Diagramme de modèle en deux étapes

Le diagramme suivant illustre le modèle de processus TwoStageApproval tel qu'il apparaît dans WorkPoint Designer. Le modèle de processus TwoStageApproval inclut trois activités manuelles :

- un noeud d'approbation pour le participant commercial. Si cet utilisateur approuve ou rejette la requête, le processus passe à l'approbateur technique ;
- un noeud d'approbation pour le participant technique. Si cet utilisateur approuve ou rejette la requête, le processus s'exécute entièrement ;
- un noeud d'approbation pour le participant par défaut. Cet utilisateur peut approuver ou rejeter la tâche si le participant commercial ou technique n'est pas trouvé ou ne répond pas.

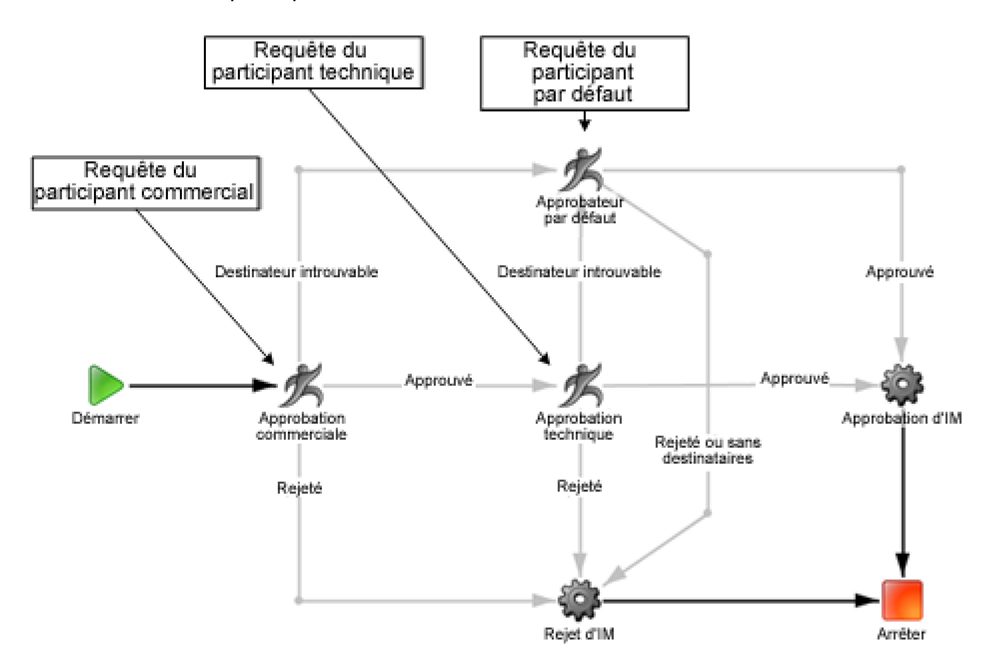
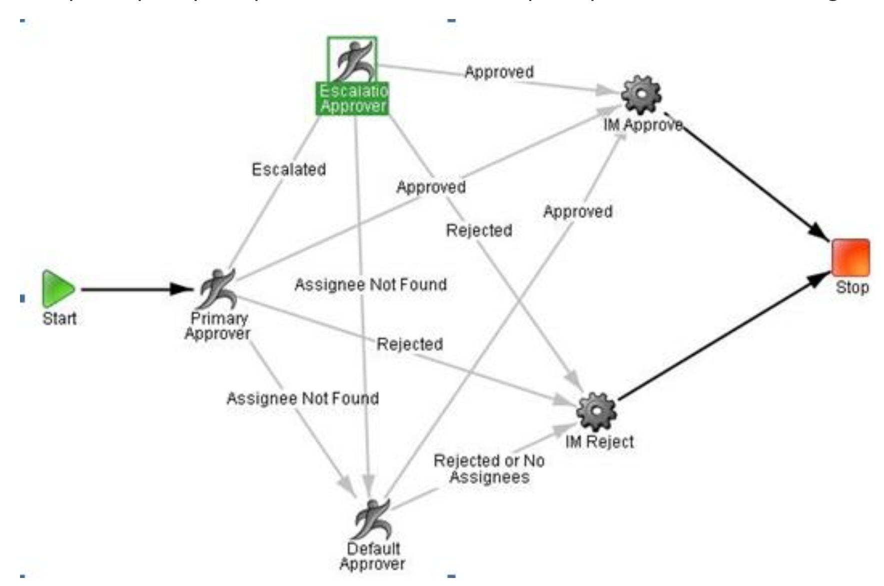


Diagramme de modèle d'approbation d'escalade

Le diagramme suivant illustre le modèle de processus EscalationApproval tel qu'il apparaît dans WorkPoint Designer. Le modèle de processus inclut les activités manuelles suivantes.

- Un noeud d'approbation pour le participant principal. Si cet utilisateur approuve ou rejette la requête, le processus s'exécute entièrement.
- Un noeud d'approbation pour un participant par défaut. Cet utilisateur peut approuver ou rejeter la requête si le participant principal est introuvable.

- Un noeud d'approbation de transition programmé de l'approbateur principal vers l'approbateur d'escalade. Cet utilisateur peut approuver ou rejeter la demande si le participant principal est trouvé, mais ne répond pas dans le délai configuré.



Remarque : Pour ajouter un délai d'expiration à un processus existant, ajoutez le champ de données d'utilisateur PARTICIPANT_TIMEOUT au noeud d'activité et ajoutez la transition Escaladé sur le noeud pour lequel vous souhaitez escalader la tâche.

Utilisation du modèle d'approbation d'escalade

Pour utiliser le modèle d'approbation d'escalade, vous devez importer manuellement le fichier .zip suivant lors de la mise à niveau de la version r12.5 à r12.5 SP1 :

Workflow 12.5 to 12.5 SP1 upgrade.zip

Ce fichier est situé dans le dossier workflowScripts sous Outils d'administration.

. Les outils d'administration sont situés aux emplacements par défaut ci-après.

- Windows : <chemin_installation>\tools
- UNIX : <chemin_installation2>/tools

Utilisation de la méthode des modèles

Cette section liste les étapes détaillées impliquées dans le placement de tâches d'administration sous le contrôle du flux de travaux selon la méthode de modèles.

Pour utiliser la méthode des modèles

1. Dans la console d'utilisateur, ouvrez la fenêtre Modifier la tâche d'administration ou Créer une tâche d'administration pour la tâche que vous souhaitez placer sous le contrôle du flux de travaux.
2. Pour implémenter le flux de travaux au niveau tâche :
   a. Dans l'onglet Profil, cliquez sur le bouton Processus de flux de travaux.
   b. dans l'onglet de configuration du flux de travaux au niveau tâche, sélectionnez un modèle de processus et configurer l'outil de résolution de participants.
3. Pour implémenter le flux de travaux au niveau événement :
   a. Dans l'onglet Evénements, sélectionnez un ou plusieurs événements ;
   b. dans l'onglet de configuration du flux de travaux au niveau événement, sélectionnez un modèle de processus et configurer l'outil de résolution de participants.
4. une fois le contrôle du flux de travaux configuré, l'utilisateur disposant du rôle approprié effectue les tâches d'administration.
5. Le participant au flux de travaux désigné approuve ou rejette la tâche ou l'événement.

Informations complémentaires :

Flux de travaux au niveau événement (page 429)
Flux de travaux de niveau tâche (page 426)
Outils de résolution de participants : méthode des modèles (page 432)

Evénements et tâches

CA IdentityMinder vous permet d'associer des processus de flux de travaux avec des tâches ou des événements. Les participants peuvent ainsi approuver ou rejeter l'intégralité de la tâche CA IdentityMinder ou un événement précis.

Par exemple, certaines tâches CA IdentityMinder générant plusieurs événements, un approbateur peut avoir besoin de consulter tous les événements avant d'approuver ou de rejeter une demande. Il est possible de le faire dans le cadre du flux de travaux au niveau tâche. Quand un processus de flux de travaux est associé à un événement précis dans une tâche, il est impossible pour l'approbateur de voir le contexte global de la tâche objet de la requête.

Flux de travaux de niveau tâche

Le flux de travaux de niveau tâche permet aux approbateurs de consulter tous les événements avant de décider d'approuver ou de rejeter une demande.

Le flux de travaux au niveau tâche se produit avant tout traitement d'une activité de tâche. Aucun événement ou tâche imbriquée ne s'exécute avant le début du job de processus de travaux.

Si le flux de travaux au niveau tâche est rejeté, aucune partie de la tâche ne s'exécute.

Vous configurez le mappage des flux de travaux au niveau tâche et les outils de résolution de participants dans l'onglet Profil pour Modifier la tâche d'administration ou Créer une tâche d'administration.

Remarque : Une tâche configurée pour le contrôle du flux de travaux au niveau tâche peut également être configurée en même temps pour le contrôle du flux de travaux au niveau événement. Un flux de travaux simultané au niveau événement peut être appliqué globalement ou à une tâche spécifique.

Informations complémentaires

Flux de travaux au niveau événement (page 429)
Mappage global de processus vers des événements (page 444)

Attribut de processus au niveau tâche

Les processus de flux de travaux qui sont compatibles avec un flux de travaux au niveau tâche ont tous un attribut spécial défini dans WorkPoint Designer. Cet attribut de données de l'utilisateur au niveau processus, appelé TASK_LEVEL, est défini par défaut sur vrai dans les modèles de processus suivants :

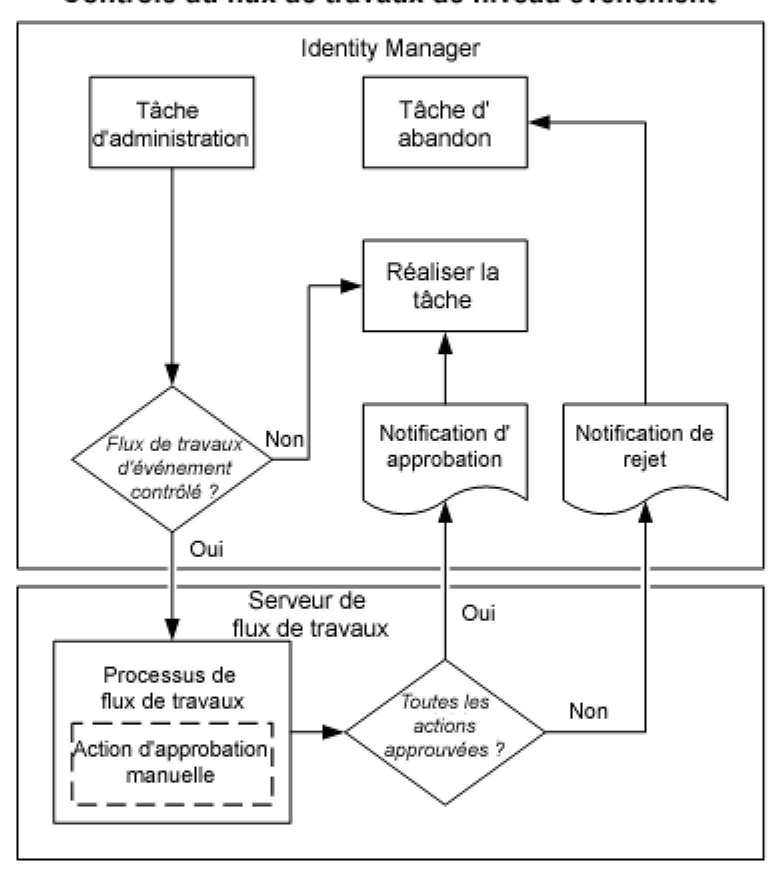
- SingleStepApproval
- TwoStageApprovalProcess

Lorsque vous sélectionnez une tâche d'administration pour un flux de travaux au niveau tâche, seuls ces modèles de processus sont disponibles.

Remarque : Même si TASK_LEVEL est défini sur vrai, il est toujours possible d'utiliser les modèles de processus pour un flux de travaux au niveau événement. Ne modifiez pas cette valeur de l'attribut TASK_LEVEL.

Diagramme de contrôle au niveau tâche

Le diagramme suivant illustre l'interaction entre CA IdentityMinder et un serveur de flux de travaux quand un processus de flux de travaux classique de niveau tâche est lancé.



Informations complémentaires :

Diagramme de contrôle au niveau événement (page 430)

Configuration d'un flux de travaux au niveau tâche

Le flux de travaux au niveau tâche se produit avant tout traitement d'une activité de tâche. Aucun événement ou tâche imbriquée ne s'exécute avant le début du job de processus de travaux.

Pour configurer un flux de travaux de niveau tâche :

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration (ou Créer une tâche d'administration).

   Une fenêtre Sélectionner une tâche d'administration apparaît.

2. Recherchez la tâche que vous souhaitez placer sous contrôle du flux de travaux et cliquez sur Sélectionner.

   Une fenêtre Modifier la tâche d'administration (ou Créer une tâche d'administration) apparaît.

3. Dans l'onglet Profil, vérifiez que l'option Activer le flux de travaux est activée.

4. Dans l'onglet Profil, cliquez sur le bouton Processus de flux de travaux.

   L'onglet Configuration du flux de travaux au niveau tâche apparaît.

5. Sélectionnez un des modèles de processus suivants dans la liste Processus de flux de travaux :

   - SingleStepApproval
   - TwoStageApprovalProcess

   L'onglet Configuration du flux de travaux au niveau tâche se développe.

6. Configurez les outils de résolution de participants selon le modèle de processus.

   Les requêtes de participants sont ajoutées selon le modèle de processus.

7. Cliquez sur OK.

   CA IdentityMinder enregistre votre configuration de flux de travaux de niveau tâche.

8. Cliquez sur Soumettre.

   CA IdentityMinder traite la modification de tâche.

Informations complémentaires :

Outils de résolution de participants : méthode des modèles (page 432)

Flux de travaux au niveau événement

Un événement CA IdentityMinder peut être mappé vers un processus de flux de travaux. Lorsqu'un événement mappé vers un processus de flux de travaux est déclenché, ce dernier commence. La tâche ayant déclenché l'événement est placée en attente et considérée comme étant sous le contrôle du flux de travaux.

Avant de pouvoir être achevé, un processus de flux de travaux peut nécessiter qu'un participant CA IdentityMinder approuve ou rejette un événement ou une tâche. Une tâche nécessitant une approbation manuelle du flux de travaux par un participant prend plus longtemps pour terminer qu'une tâche ne se trouvant pas sous le contrôle d'un flux de travaux.

Lorsque toutes les activités d'un processus de flux de travaux ont été effectuées, l'événement mappé vers le processus de flux de travaux est libéré du contrôle de flux de travaux. Lorsque tous les événements déclenchés par une tâche donnée sont libérés du contrôle de flux de travaux, la tâche contrôlée par le flux de travaux est terminée.

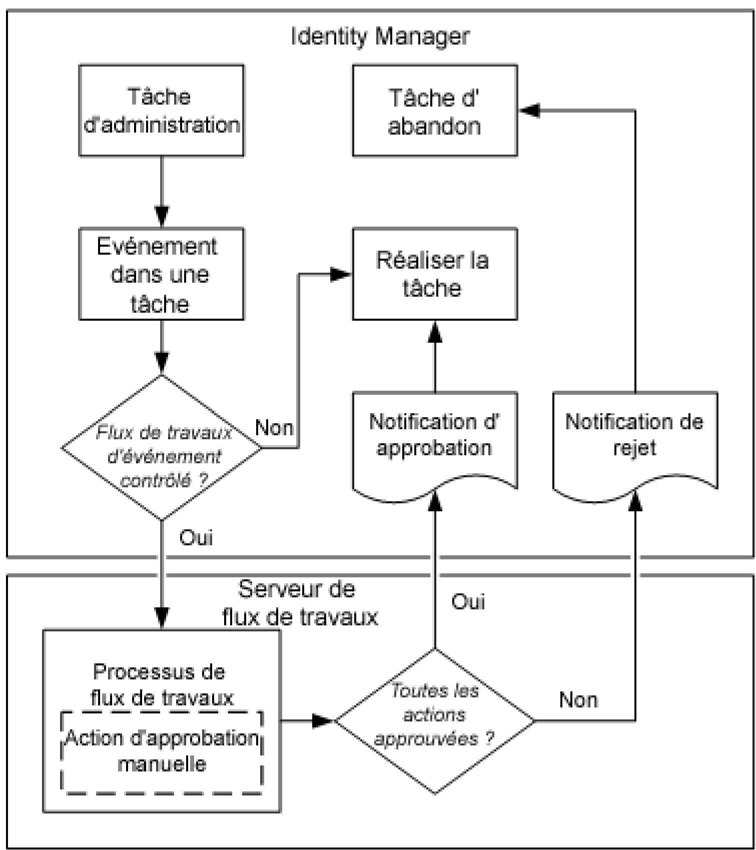
Tant que la tâche est sous le contrôle du flux de travaux, le contenu des écrans de tâches est enregistré dans la base de données de persistance des tâches. L'état du job de flux de travaux (données correspondant au flux de travaux) est enregistré dans la base de données WorkPoint.

Vous configurez le mappage des flux de travaux au niveau événement et les outils de résolution de participants dans l'onglet Evénements pour Modifier la tâche d'administration ou Créer une tâche d'administration.

Remarque : L'onglet Evénements répertorie les événements générés par chaque onglet d'une tâche. Après avoir ajouté un nouvel onglet à une tâche, vous devez soumettre puis rouvrir la tâche à l'aide de la tâche Modifier la tâche d'administration avant l'affichage des nouveaux événements dans l'onglet Evénements.

Diagramme de contrôle au niveau événement

Le diagramme suivant présente l'interaction entre CA IdentityMinder et le serveur de flux de travaux lorsqu'un processus de flux de travaux classique de niveau événement est lancé.



Informations complémentaires :

Diagramme de contrôle au niveau tâche (page 427)

Configuration d'un flux de travaux au niveau événement

Le flux de travaux au niveau événement commence quand un événement mappé vers un processus de flux de travaux est déclenché. La tâche ayant déclenché l'événement est placée en attente jusqu'à ce que le participant approuve ou rejette la tâche.

Pour configurer un flux de travaux de niveau événement :

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration (ou Créer une tâche d'administration).

   Une fenêtre Sélectionner une tâche d'administration apparaît.

2. Recherchez la tâche que vous souhaitez placer sous contrôle du flux de travaux et cliquez sur Sélectionner.

   Une fenêtre Modifier la tâche d'administration (ou Créer une tâche d'administration) apparaît.

3. Dans l'onglet Profil, vérifiez que l'option Activer le flux de travaux est activée.

4. Dans l'onglet Evénements, sélectionnez un événement à mapper vers un modèle de processus.

   La fenêtre de mappage du flux de travaux apparaît.

5. Sélectionnez un des modèles de processus suivants dans la liste Processus de flux de travaux :

   - SingleStepApproval
   - TwoStageApprovalProcess

   La fenêtre de mappage du flux de travaux apparaît.

6. Configurez les outils de résolution de participants selon le modèle de processus.

   Les requêtes de participants sont ajoutées selon le modèle de processus.

7. Cliquez sur OK.

   CA IdentityMinder enregistre votre configuration de flux de travaux de niveau événement.

8. Répétez les étapes 3 à 6 pour chaque événement que vous souhaitez placer sous le contrôle du flux de travaux.

9. Cliquez sur Soumettre.

   CA IdentityMinder traite la modification de tâche.

Remarque : La liste de processus de flux de travaux comprend des processus à utiliser selon la méthode des modèles et la méthode WorkPoint :

- quand un processus de méthode de modèles est sélectionné (SingleStepApproval ou TwoStageApprovalProcess), la page se développe pour permettre la configuration de l'outil de résolution de participants ;
- quand un processus de méthode WorkPoint est sélectionné, la page ne se développe pas. Les outils de résolution de participants se configurent dans WorkPoint Designer.

Informations complémentaires :

Outils de résolution de participants : méthode des modèles (page 432)

Outils de résolution de participants : méthode des modèles

Pour spécifier des participants au moyen de la méthode des modèles de processus, vous définissez les propriétés de l'activité suivantes dans la console d'utilisateur :

- le nom de la tâche d'approbation ;
- le type d'outil de résolution de participants ;
- L'outil de résolution de participants nécessite des informations supplémentaires.

Les outils de résolution de participants sont configurés dans les écrans suivants de la console d'utilisateur :

Flux de travaux de niveau tâche

Fenêtre de configuration des flux de travaux, sélectionnée dans l'onglet Profil de Modifier la tâche d'administration ou Créer une tâche d'administration.

Flux de travaux de niveau événement

Fenêtre de configuration des flux de travaux, sélectionnée dans l'onglet Profil de Modifier la tâche d'administration ou Créer une tâche d'administration.

Types d'outils de résolution de participants

Pour la méthode des modèles, il existe sept types d'outils de résolution de participants :

Membres du rôle de la tâche d'approbation

Spécifie que les participants sont membres des rôles qui autorisent l'accès à la tâche d'approbation.

Liste des utilisateurs

Spécifie que les participants font partie d'une liste d'utilisateurs.

Membres du groupe

Spécifie que les participants sont membres d'une liste de groupes.

Membres du rôle d'administration

Spécifie que les participants sont membres d'une liste de groupes.

Membres de la tâche d'administration

Spécifie que les participants sont membres de rôles d'administration associés à une liste de tâches d'administration.

Outil de résolution dynamique

Spécifie que les participants sont sélectionnés de manière dynamique selon la tâche ou l'événement approuvé.

Outil de résolution nul

Renvoie une liste vide sans utilisateur.

Personnalisé

Spécifie que les participants sont déterminés selon un outil de résolution de participants personnalisé.

Stratégie de messagerie électronique

Vous pouvez spécifier une stratégie de messagerie électronique pour chaque étape du processus de flux de travaux. Selon la stratégie de messagerie électronique définie, un courriel est envoyé lorsqu'un processus atteint l'étape ou l'activité correspondante. Pour les courriels de notification relatifs aux processus de flux de travaux, vous pouvez uniquement sélectionner le type *Planification de l'envoi* : *Flux de travaux en attente de spécification de l'adresse électronique*.

Pour plus d'informations sur les stratégies de messagerie électronique, consultez la section Procédure de création de stratégies de notification par courriel.

Membres du rôle de la tâche d'approbation

Cet outil de résolution affecte l'activité à tous les membres des rôles CA IdentityMinder qui accordent l'autorisation d'accès à la tâche d'approbation. Cet outil de résolution ne nécessite aucune autre configuration.

Pour configurer un outil de résolution de membres du rôle de la tâche d'approbation

1. Dans l'écran de configuration du flux de travaux de la console d'utilisateur, sélectionnez Membres du rôle de la tâche d'approbation dans la liste d'outils de résolution de participants.

   La fenêtre de configuration du flux de travaux se modifie selon la sélection de l'outil de résolution de participants.

2. Cliquez sur OK pour enregistrer la configuration de l'outil de résolution de participants.

   L'onglet Profil de tâche d'administration réapparaît.

3. Cliquez sur Soumettre pour enregistrer les modifications de votre flux de travaux de tâche d'administration.

Liste des utilisateurs

Cet outil de résolution affecte la tâche à une liste d'utilisateurs spécifiés.

La portée n'est pas appliquée. Quiconque ayant accès à l'écran de configuration du flux de travaux peut ajouter ou supprimer un utilisateur de la liste.

Cet outil de résolution a les règles de validation suivantes :

- vous devez spécifier au moins un nom d'utilisateur ;
- les noms d'utilisateur doivent être ceux d'utilisateurs existant actuellement.

Pour configurer un outil de résolution de liste d'utilisateurs

1. Dans l'écran de configuration du flux de travaux de la console d'utilisateur, sélectionnez Liste d'utilisateurs dans la liste d'outils de résolution de participants.

   La fenêtre de configuration du flux de travaux se modifie selon la sélection de l'outil de résolution de participants.

2. Cliquez sur Ajouter l'utilisateur pour ajouter un participant à la liste.

   Une fenêtre de sélection des utilisateurs apparaît.

3. Cherchez et sélectionnez un ou plusieurs participants.

   Les participants sont ajoutés à la liste d'utilisateurs.

4. Cliquez sur OK pour enregistrer la configuration de l'outil de résolution de participants.

   L'onglet Profil de tâche d'administration réapparaît.

5. Cliquez sur Soumettre pour enregistrer les modifications de votre flux de travaux de tâche d'administration.

Membres du groupe

Cet outil de résolution affecte la tâche à tous les membres de tous les groupes spécifiés dans la liste de groupes.

L'évaluation de qui sont les membres du groupe s'effectue en même temps que la tâche est créée, pas quand l'outil de résolution de participants est spécifié.

La portée n'est pas appliquée. Quiconque ayant accès à l'écran de configuration du flux de travaux peut ajouter ou supprimer un groupe de la liste.

Cet outil de résolution a les règles de validation suivantes :

- Vous devez spécifier au moins un nom de groupe.
- Les noms de groupes doivent être ceux de groupes existant actuellement.

Pour configurer un outil de résolution de membres de groupe

1. Dans l'écran de configuration du flux de travaux de la console d'utilisateur, sélectionnez Liste d'utilisateurs dans la liste d'outils de résolution de participants.

   La fenêtre de configuration du flux de travaux se modifie selon la sélection de l'outil de résolution de participants.

2. Cliquez sur Ajouter des groupes pour ajouter un groupe à la liste.

   Une fenêtre de sélection des utilisateurs apparaît.

3. Cherchez et sélectionnez un ou plusieurs groupes.

   Les groupes sont ajoutés à la liste de groupes.

4. Cliquez sur OK pour enregistrer la configuration de l'outil de résolution de participants.

   L'onglet Profil de tâche d'administration réapparaît.

5. Cliquez sur Soumettre pour enregistrer les modifications de votre flux de travaux de tâche d'administration.

Membres du rôle d'administration

Cet outil de résolution affecte la tâche à tous les membres des rôles d'administration spécifiés dans la liste de rôles d'administration.

L'identification des membres de rôle est effectuée lors de la création de la tâche et non lors de la spécification de l'outil de résolution de participants.

La portée n'est pas appliquée. Les utilisateurs ayant accès à la fenêtre de configuration du flux de travaux peuvent ajouter ou supprimer un rôle dans la liste.

Cet outil de résolution inclut les règles de validation suivantes :

- Au moins un rôle d'administration doit être spécifié.
- Les noms de rôle d'administration doivent correspondre aux noms des rôles d'administration existants.

Pour configurer un outil de résolution de membres du rôle d'administration :

1. Dans la fenêtre de configuration du flux de travaux de la console d'utilisateur, sélectionnez Membres du rôle d'administration dans la liste Outil de résolution de participants.

   La fenêtre de configuration du flux de travaux se modifie selon la sélection de l'outil de résolution de participants.

2. Cliquez sur Ajouter des rôles d'administration pour ajouter un rôle à la liste.

   Une fenêtre de sélection des rôles apparaît. Elle inclut une case à cocher permettant d'activer la portée des rôles que vous ajoutez.

3. Recherchez et sélectionnez un ou plusieurs rôles.

   Les rôles sélectionnés sont ajoutées à la liste des rôles

4. Sélectionnez la case à cocher Forcer les règles de portée si vous voulez appliquer des règles de portée.

5. Cliquez sur OK pour enregistrer la configuration de l'outil de résolution de participants.

   L'onglet Profil de tâche d'administration réapparaît.

6. Cliquez sur Soumettre pour enregistrer les modifications de votre flux de travaux de tâche d'administration.

Membres de la tâche d'administration

Cet outil de résolution affecte la tâche à tous les membres des rôles d'administration associés aux tâches d'administration figurant dans la liste de rôles d'administration.

La portée n'est pas appliquée. Quiconque ayant accès à l'écran de configuration du flux de travaux peut ajouter ou supprimer une tâche de la liste.

L'évaluation de qui sont les membres du rôle et quels rôles sont présents pour les tâches s'effectue en même temps que la tâche est créée, pas quand l'outil de résolution de participants est spécifié.

Cet outil de résolution a les règles de validation suivantes :

- Vous devez spécifier au moins une tâche d'administration.
- Les noms des tâches d'administration doivent être ceux de tâches d'administration existant actuellement.

Pour configurer un outil de résolution de tâches du rôle d'administration

1. Dans l'écran de configuration du flux de travaux de la console d'utilisateur, sélectionnez Membres du rôle de la tâche d'approbation dans la liste d'outils de résolution de participants.

   La fenêtre de configuration du flux de travaux se modifie selon la sélection de l'outil de résolution de participants.

2. Cliquez sur Ajouter des tâches d'administration pour ajouter une tâche à la liste.

   Une fenêtre Sélectionner une tâche d'administration apparaît.

3. Cherchez et sélectionnez une ou plusieurs tâches.

   Les tâches sont ajoutées à la liste de tâches.

4. Cliquez sur OK pour enregistrer la configuration de l'outil de résolution de participants.

   L'onglet Profil de tâche d'administration réapparaît.

5. Cliquez sur Soumettre pour enregistrer les modifications de votre flux de travaux de tâche d'administration.

Outil de résolution dynamique

Cet outil de résolution renvoie une liste d'utilisateurs selon une règle dynamique à l'exécution. Utilisez la sélection suivante pour définir des contraintes de règles dynamiques.

Approbateurs

Spécifie le type d'utilisateur qui approuve cette tâche.

Remarque : Seuls les objets pouvant contenir des utilisateurs (ou des approbateurs) s'affichent.

Utilisateur ou Objet

Spécifie l'utilisateur ou l'objet contenant les approbateurs.

- Objet associé à l'événement : événement sous le contrôle de flux de travaux.
- Auteur de la tâche : utilisateur qui a initié la tâche d'administration.
- Objet principal de la tâche : objet créé/modifié par la tâche.
- Approbateur précédent de la tâche : approbateurs précédents de la tâche.

Attribut

Spécifie l'attribut contenant les approbateurs.

Type d'objet d'événement

Spécifie le type d'objet de l'événement.

Remarque : Ce type apparaît uniquement si l'option Objet associé à l'événement est sélectionnée.

L'outil de résolution a été amélioré pour ajouter un précédent approbateur à la liste des objets pris en charge. Si l'attribut physique hébergeant les informations sur le gestionnaire est sélectionné, la configuration achemine une approbation vers un gestionnaire.

Pour configurer l'outil de résolution des approbations de gestionnaires

- Définissez les approbateurs sur Utilisateurs.
- Sélectionnez Utilisateur ou Objet.
- Définissez l'attribut sur un attribut physique contenant les informations sur le gestionnaire.

L'ajout de l'approbateur précédent à la liste des objets pris en charge de l'outil de résolution permet d'utiliser l'outil de résolution dynamique avec le processus d'approbation d'escalade. Etant donné que la modification est uniquement effectuée pour l'utilisation du processus d'approbation d'escalade, il n'existe pas de distinction de la personne ayant effectivement effectué l'approbation. L'ensemble des UTILISATEURS identifiés en tant qu'approbateurs pour la tâche précédente du job en cours sont examinés pour obtenir l'information requise (ID unique du gestionnaire, etc.). Tous les individus identifiés par cette inspection sont les approbateurs de la tâche actuelle (escalade).

Outil de résolution de correspondance d'attribut

Cet outil fonctionne uniquement avec les objets de type Utilisateur. Une valeur de n'importe quel objet disponible est mise en correspondance avec un champ de l'objet Utilisateur. Utilisez la sélection suivante pour définir des contraintes de règles de correspondance d'attribut.

Approbateurs

Spécifie le type d'utilisateur qui approuve cette tâche.

Utilisateur ou Objet

Spécifie la valeur affichée pour les approbateurs dans l'attribut sélectionné ci-dessous.

Remarque : La valeur extraite de l'utilisateur ou de l'objet doit être une valeur acceptable pour une recherche d'utilisateur pour l'attribut sélectionné.

- Objet associé à l'événement : événement sous le contrôle d'un flux de travaux.
- Auteur de la tâche : utilisateur qui a initié la tâche d'administration.
- Objet principal de la tâche : objet créé/modifié par la tâche (uniquement disponible pour le mappage d'événements de niveau tâche.)
- Approbateur précédent de la tâche : approbateurs précédents de la tâche.

Attribut d'utilisateur ou d'objet

Spécifie l'attribut qui contient la valeur à utiliser dans la recherche d'approbateurs.

Attribut de recherche de l'approbateur

Spécifie l'attribut utilisé dans la recherche à faire correspondre avec la valeur identifiée ci-dessus.

Pour qu'ils soient disponibles, vous devez importer les scripts de mise à niveau pour le processus d'approbation d'escalade des informations d'approbateur précédentes (UpgradeWFScripts.zip). Importez les scripts du dossier workflowScripts dans les outils d'administration aux emplacements par défaut suivants :

- Windows : <chemin_d'installation>\tools
- UNIX : <chemin_d'installation2>/tools

Lors de l'importation de scripts WorkPoint avec l'outil d'archivage lors de la mise à niveau, l'administrateur doit spécifier qu'il s'agit d'une importation dans une base de données existante et remplacer les scripts existants.

Remarque : Lorsque vous définissez la tâche "Approuver la création d'un utilisateur" en tant qu'outil de résolution de correspondance d'attribut s'appliquant aux utilisateurs et à l'outil de résolution de participants, vous devez changer la signature de méthode pour le script imApprovers dans Workpoint Designer de manière à pointer sur le nom unique de TwoStageProcessDefinition.

Outil de résolution nul

L'outil de résolution nul ne retourne aucun utilisateur. De ce fait, selon la conception du processus de flux de travaux, le processus peut ignorer totalement l'approbation. L'outil de résolution nul ne nécessite aucune autre configuration.

Pour configurer un outil de résolution nul

1. Dans l'écran de configuration du flux de travaux de la console d'utilisateur, sélectionnez Liste d'utilisateurs dans la liste d'outils de résolution de participants.

   La fenêtre de configuration du flux de travaux se modifie selon la sélection de l'outil de résolution de participants.

2. Cliquez sur OK pour enregistrer la configuration de l'outil de résolution de participants.

   L'onglet Profil de tâche d'administration réapparaît.

3. Cliquez sur Soumettre pour enregistrer les modifications de votre flux de travaux de tâche d'administration.

Outil de résolution de participants personnalisé

L'outil de résolution de participants personnalisé est un objet Java qui détermine les participants à l'activité de flux de travaux et renvoie une liste à CA IdentityMinder, qui la transmet au moteur de flux de travaux. En général, vous écrivez uniquement un outil de résolution personnalisé si les stratégies de participant standard ne peuvent pas fournir la liste des participants requis pour une activité.

Remarque : Vous pouvez créer un outil de résolution personnalisé au moyen de l'outil de résolution de participants API. Pour plus d'informations, reportez-vous au *manuel de programmation Java (en anglais).*

Pour configurer un outil de résolution personnalisé

1. Dans la fenêtre de configuration du flux de travaux de la console d'utilisateur, sélectionnez Personnaliser : *<nom de l'outil de résolution>* dans la liste des outils de résolution de participants.

   La fenêtre de configuration du flux de travaux se modifie selon la sélection de l'outil de résolution de participants.

2. Ajoutez les paramètres d'entrée requis par votre outil de résolution de participants personnalisé.

3. Cliquez sur OK pour enregistrer la configuration de l'outil de résolution de participants.

   L'onglet Profil de tâche d'administration réapparaît.

4. Cliquez sur Soumettre pour enregistrer les modifications de votre flux de travaux de tâche d'administration.

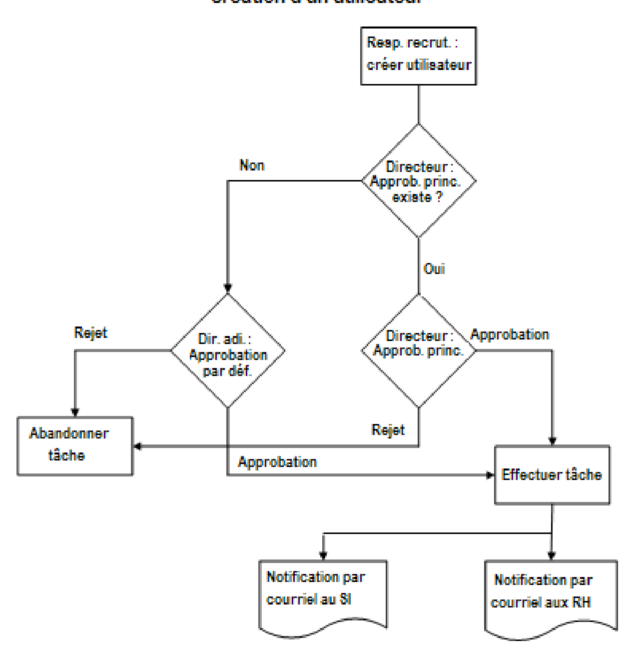
Exemple de flux de travaux : Créer un utilisateur

Un administrateur CA IdentityMinder de la société doit définir un flux de travaux et des rôles d'utilisateurs pour traiter le scénario suivant.

- le Chef des ventes engage un nouveau Représentant. Le Chef des ventes doit être en mesure de créer un utilisateur CA IdentityMinder pour le nouvel employé.
- pour rationaliser le processus d'embauche, les participants veulent effectuer uniquement une tâche pour approuver (ou rejeter) la tâche ;
- le Responsable commercial devrait être le principal approbateur pour tous les nouveaux employés. Si le Responsable commercial est incapable de le faire, le Directeur Commercial devrait être l'approbateur par défaut.
- Si le nouvel employé est approuvé, CA IdentityMinder doit envoyer des courriels de notification aux départements Ressources Humaines (RH) et Services Informatiques (SI).

Diagramme de contrôle de la création d'un utilisateur

Le diagramme suivant illustre le flux logique pour le scénario de création d'un utilisateur.



Implémentation d'un exemple de flux de travaux

Pour implémenter ce scénario d'exemple, l'administrateur nécessite d'effectuer les tâches suivantes :

- Il doit s'assurer que l'auteur de la tâche est membre du rôle d'administration requis.

  le Chef des ventes doit être membre du rôle administratif de gestionnaire d'utilisateur. Ce rôle donne l'autorité requise au Chef des ventes pour commencer la tâche administrative Créer un utilisateur afin d'embaucher un nouveau Représentant.

- Il doit activer un flux de travaux de niveau tâche pour la tâche d'administration Créer un utilisateur.

  Le flux de travaux au niveau tâche garantit que seule une tâche est générée pour terminer la tâche Créer un utilisateur. Etant donné qu'il existe plusieurs événements individuels associés à la tâche Créer un utilisateur, un flux de travaux au niveau événement générerait plusieurs tâches et serait aussi plus difficile à configurer.

- Configuration des outils de résolution de participants

  Le nombre d'outils de résolution de participants possibles est déterminé par le modèle de processus de flux de travaux sélectionné. Le modèle SingleStageApproval inclut des approbateurs principaux et par défaut, d'autres modèles en autorisant plus.

  Puisque ce scénario requiert uniquement deux approbateurs, l'outil de résolution de participants de la liste des utilisateurs constitue la solution la plus simple. Cet outil de résolution permet à des approbateurs individuels d'être sélectionnés par nom plutôt que plusieurs utilisateurs par rôle ou groupe.

- Configuration de courriels de notification

  La console de gestion permet des courriels de notification pour des tâches et événements spécifiques. Pour ce scénario, la tâche de courriel est activée et des courriels de notification sont envoyés quand la tâche Créer un utilisateur s'achève.

  Un modèle de courriel personnalisé est requis pour envoyer un courriel aux départements RH et SI avec la ligne d'objet et le texte du message correspondants.

Informations complémentaires

Utilisation de la méthode des modèles (page 424)
Configuration d'un flux de travaux au niveau tâche (page 428)
Outils de résolution de participants : méthode des modèles (page 432)
Notifications par courriel (page 515)

Méthode WorkPoint

La méthode WorkPoint s'appliquait aux versions d'CA IdentityMinder antérieures à la version r12. 14 processus de flux de travaux WorkPoint prédéfinis sont mappés par défaut vers des événements CA IdentityMinder. Vous devez utiliser WorkPoint Designer pour configurer les outils de résolution de participants et, dans le cas contraire, modifier les processus de flux de travaux.

La méthode WorkPoint nécessite également que vous utilisiez la console de gestion CA IdentityMinder pour mapper une procédure de flux de travaux vers un événement d'approbation pour placer la tâche correspondante sous le contrôle d'un flux de travaux à un niveau global au sein de l'environnement.

Utilisation de la méthode Workpoint

Cette section liste les étapes détaillées impliquées dans le placement de tâches d'administration sous le contrôle du flux de travaux selon la méthode de modèles WorkPoint.

Remarque : Pour une meilleure souplesse et commodité, CA vous recommande d'utiliser la méthode des modèles dans la mesure du possible.

Pour utiliser la méthode Workpoint

1. Dans la console de gestion :
   a. Veillez à ce que le flux de travaux soit activé.
   b. (Facultatif) Pour un mappage global d'événements, associez un ou plusieurs événements au processus de flux de travaux prédéfini approprié.
   c. Si nécessaire, redémarrez l'environnement CA IdentityMinder.
2. Dans la console d'utilisateur :
   a. pour un mappage d'événements propre à une tâche, associez un ou plusieurs événements au processus de flux de travaux prédéfini approprié (facultatif).
3. Dans WorkPoint Designer :
   a. associez une tâche d'approbation avec un processus de flux de travaux (facultatif) ;
   b. configurez des outils de résolution de participants avec un processus de travaux (facultatif)
4. Dans la console d'utilisateur :
   a. une fois le contrôle du flux de travaux configuré, l'utilisateur disposant du rôle approprié effectue les tâches d'administration.
   b. Le participant au flux de travaux désigné approuve ou rejette l'événement.

Informations complémentaires :

Mappage de processus vers des événements (page 445)
Associer une activité de flux de travaux à une tâche d'approbation. (page 450)
Outils de résolution de participants : méthode Workpoint (page 452)

Processus WorkPoint

CA IdentityMinder inclut plusieurs processus de flux de travaux prédéfinis dans WorkPoint Designer. Vous pouvez utiliser les processus prédéfinis avec leurs mappages d'événements par défaut, mapper les processus de flux de travaux vers d'autres événements, modifier ces processus en ajoutant ou en supprimant des activités et en créer des nouveaux.

Mappage global de processus vers des événements

Le mappage d'un processus de flux de travaux vers un événement à un niveau global peut éventuellement utiliser une stratégie.

Pour plus d'informations sur la procédure de mappage d'un événement vers un processus de flux de travaux à l'aide d'un flux de travaux utilisant une stratégie, reportez-vous à la rubrique Mappage de flux de travaux utilisant une stratégie globale de niveau événement.

Ce tableau montre les mappages globaux par défaut d'événements et de processus de flux de travaux spécifiés dans la console de gestion.

Important : Il s'agit de mappages globaux. Le processus de flux de travaux mappé s'exécute chaque fois que l'événement correspondant est généré par une tâche quelconque dans l'environnement.

Processus de flux de travaux	Événement mappé
CertifyRoleApproveProcess	CertifyRoleEvent
CreateGroupApproveProcess	CreateGroupEvent
CreateOrganizationApproveProcess	CreateOrganizationEvent
CreateUserApproveProcess	CreateUserEvent
DeleteGroupApproveProcess	DeleteGroupEvent
DeleteOrganizationApproveProcess	DeleteOrganizationEvent
DeleteUserApproveProcess	DeleteUserEvent
ModifyAccessRoleMembershipApproveProcess	AssignAccessRoleEvent RevokeAccessRoleEvent
ModifyAdminRoleMembershipApproveProcess*	
ModifyGroupMembershipApproveProcess*	
ModifyOrganizationApproveProcess	ModifyOrganizationEvent
SelfRegistrationApproveProcess	SelfRegisterUserEvent

Remarque : Les processus de flux de travaux marqués avec un astérisque (*) ne sont pas mappés vers des événements par défaut.

Informations complémentaires :

Mapper un processus vers un événement globalement (page 446)
Mapper un processus vers un événement dans une tâche spécifique (page 447)

Mappage de processus vers des événements

Vous créez et modifiez des processus de flux de travaux dans WorkPoint Designer. Lorsque vous créez un processus de flux de travaux pour CA IdentityMinder, vous avez en tête une tâche de CA IdentityMinder. L'exécution de cette tâche est contrôlée par le processus de flux de travaux.

Outre la création du processus de flux de travaux, vous devez également effectuer les opérations ci-dessous.

- Identifiez l'événement généré par la tâche CA IdentityMinder, décrite dans Evénements et Tâches d'administration. Vous pouvez créer un processus de flux de travaux pour toute tâche d'CA IdentityMinder générant un événement.
- Mappez le processus de flux de travaux vers un événement en procédant de l'une des manières suivantes :
  - Affecter globalement un processus de flux de travaux à un événement.

    Avec ce mappage global, le processus de flux de travaux se produit chaque fois qu'un événement est généré dans l'environnement, quelle que soit la tâche générant l'événement.
  - Affecter un processus de flux de travaux à un événement généré par une tâche spécifique.

    Avec ce mappage spécifique à la tâche, le processus de flux de travaux se produit uniquement lorsque la tâche spécifiée génère l'événement.

  Remarque : Si vous mappez un événement vers un processus de flux de travaux, tous deux globalement et vers une tâche spécifique, le processus de flux de travaux associé à la tâche spécifique est prioritaire.
- Spécifier un outil de résolution pour l'activité de flux de travaux dans le processus de flux de travaux.
- Associer une activité de flux de travaux à une tâche d'approbation.

Informations complémentaires :

Mapper un processus vers un événement globalement (page 446)
Mapper un processus vers un événement dans une tâche spécifique (page 447)
Activités de flux de travaux (page 449)
Outils de résolution de participants : méthode Workpoint (page 452)

Mapper un processus vers un événement globalement

Vous mappez un processus de flux de travaux vers un événement globalement, afin que le processus de flux de travaux s'exécute lorsque l'événement est généré par une tâche quelconque dans l'environnement.

Pour mapper un processus de flux de travaux vers un événement globalement

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur.

   ```
   http://hostname/iam/immanage
   ```

   hostname

   Définit le nom de domaine complet du serveur sur lequel CA IdentityMinder est installé. Par exemple, monserveur.masociété.com:port.

2. Cliquez sur Environnements, puis sélectionnez le nom de l'environnement CA IdentityMinder approprié.
3. Cliquez sur Paramètres avancés puis sur Flux de travaux.
4. Procédez comme suit pour mapper un événement vers un processus de flux de travaux :
   a. Sélectionnez un événement dans la zone de liste Evénement.
   b. Sélectionnez un processus de flux de travaux dans la zone de liste Processus d'approbation.
   c. Cliquez sur Ajouter.
5. Une fois que vous avez terminé de mapper des événements vers des processus de flux de travaux, cliquez sur Enregistrer.
6. Redémarrez l'environnement CA IdentityMinder pour que les modifications soient prises en compte.

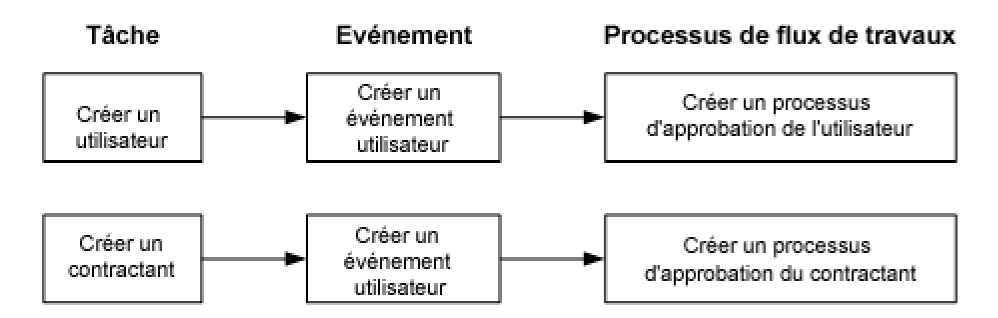
Informations complémentaires :

Mappage global de processus vers des événements (page 444)

Mapper un processus vers un événement dans une tâche spécifique

Vous pouvez affecter un processus de flux de travaux à un événement généré par une tâche particulière. Dans ce cas, le processus de flux de travaux se produit uniquement lorsque l'événement mappé est généré par la tâche spécifiée.

Le mappage spécifique à la tâche fournit un contrôle variable sur les processus de travaux qui peuvent être exécutés pour le même événement. Par exemple, le diagramme suivant montre deux tâches différentes, qui génèrent le même événement mais déclenche deux processus de flux de travaux :



Dans ce diagramme, chaque tâche utilise un processus de flux de travaux distinct.

Créer un utilisateur

Spécifie la tâche d'administration par défaut qui déclenche l'événement CreateUserEvent, qui est mappé vers le processus de flux de travaux CreateUserApproveProcess.

Créer un sous-traitant

Spécifie une tâche personnalisée basée sur la tâche Créer un utilisateur. Dans ce cas, CreateUserEvent est mappé vers CreateContractorApproveProcess, un processus de flux de travaux personnalisé créé pour l'approbation de nouveaux comptes d'entrepreneurs.

Pour mapper un processus de flux de travaux vers un événement dans une tâche existante

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
2. Rechercher une tâche d'administration
3. Sélectionnez une tâche (par exemple, les tâches Modifier l'utilisateur ou Créer un utilisateur) et cliquez sur Sélectionner.

4. Dans l'onglet Evénements, sélectionnez un processus de flux de travaux pour l'événement dans la tâche.

   Remarque : le processus de flux de travaux doit être activé pour que les noms d'événements et le menu déroulant des processus de flux de travaux apparaissent dans cet onglet.

5. Avec le menu déroulant des processus de flux de travaux, affectez un processus de flux de travaux au nom de l'événement et cliquez sur OK.
6. Cliquez sur Soumettre.
7. Ouvrez la console de gestion et redémarrez l'environnement CA IdentityMinder pour que les modifications soient prises en compte.

Pour mapper un processus de flux de travaux vers un événement dans une nouvelle tâche

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Créer une tâche d'administration.

   Remarque : Assurez-vous de sélectionner une tâche d'approbation de processus de flux de travaux (comme Approuver la création d'un groupe ou Approuver la création d'un utilisateur) en tant que modèle pour votre nouvelle tâche d'approbation de processus de flux de travaux .

2. Dans l'onglet Profil, saisissez les informations dans les champs appropriés.
3. Dans l'onglet Evénements, sélectionnez un processus de flux de travaux pour l'événement dans la tâche.

   Remarque : le processus de flux de travaux doit être activé pour que les noms d'événements et le menu déroulant des processus de flux de travaux apparaissent dans cet onglet.

4. Avec le menu déroulant des processus de flux de travaux, affectez un processus de flux de travaux au nom de l'événement et cliquez sur OK.
5. Cliquez sur Soumettre.
6. Ouvrez la console de gestion et redémarrez l'environnement CA IdentityMinder pour que les modifications soient prises en compte.

Remarque : La liste de processus de flux de travaux comprend des processus à utiliser selon la méthode des modèles et la méthode WorkPoint :

- quand un processus de méthode de modèles est sélectionné (SingleStepApproval ou TwoStageApprovalProcess), la page se développe pour permettre la configuration de l'outil de résolution de participants ;
- quand un processus de méthode WorkPoint est sélectionné, la page ne se développe pas. Les outils de résolution de participants se configurent dans WorkPoint Designer.

Informations complémentaires :

Mappage global de processus vers des événements (page 444)

Activités de flux de travaux

CA IdentityMinder inclut un certain nombre d'activités de flux de travaux prédéfinies dans WorkPoint Designer. Ces activités sont affectées aux processus de flux de travaux prédéfinis.

Les processus de flux de travaux prédéfinis sont des processus en une seule étape, c'est à dire que chaque processus se compose d'une seule activité prédéfinie.

Chaque activité prédéfinie correspond à une tâche d'approbation de flux de travaux portant le même nom, qui est prédéfinie dans CA IdentityMinder. Vous pouvez utiliser les activités prédéfinies dans d'autres processus de flux de travaux et vous pouvez créer de nouvelles activités.

Vous pouvez utiliser les processus de flux de travaux prédéfinis sans modification ou y ajouter plus d'activités. Pour plus d'informations sur l'ajout d'une activité à un processus de flux de travaux, reportez-vous à la documentation de WorkPoint.

Processus, tâches et activités

Le tableau suivant liste les activités de flux de travaux prédéfinis et les processus de flux de travaux auxquels chaque activité est affectée par défaut.

Remarque : Les activités de flux de travaux prédéfinies et les tâches correspondantes d'approbation de flux de travaux portent le même nom.

Processus de flux de travaux	Tâche Flux de travaux/Activité
CertifyRoleApprovalProcess**	Approuver la certification d'un rôle
Processus de consultation*	
CreateGroupApproveProcess	Approuver la création d'un groupe
CreateOrganizationApproveProcess	Approuver la création d'une organisation
CreateUserApproveProcess	Approuver la création d'un utilisateur
DeleteGroupApproveProcess	Approuver la suppression d'un groupe
DeleteOrganizationApproveProcess	Approuver la suppression d'une organisation
DeleteUserApproveProcess	Approuver la suppression d'un utilisateur

Processus de flux de travaux	Tâche Flux de travaux/Activité
ModifyAccessRoleMembershipApproveProcess	Approuver la modification de l'appartenance à un rôle d'accès
ModifyAdminRoleMembershipApproveProcess	Approuver la modification de l'appartenance à un rôle d'administration
ModifyGroupMembershipApproveProcess	Approuver la modification de l'appartenance à un groupe
ModifyIdentityPolicySetApproveProcess	Approuver la modification d'un ensemble de stratégies d'identité
ModifyOrganizationApproveProcess	Approuver la modification d'une organisation
ModifyUserApproveProcess	Approuver la modification d'un utilisateur
SelfRegistrationApproveProcess	Approuver l'auto-enregistrement
SingleStepApproval*	
TwoStageApprovalProcess*	

Remarque : Les processus de flux de travaux marqués avec un astérisque (*) sont conçus pour être utilisés avec la méthode des modèles. Ils sont configurés dans la console d'utilisateur et n'ont aucune tâche ou activité associée par défaut. Le CertifyRoleApprovalProcess (**) est un exemple de processus, qui fait la démonstration d'un outil de résolution de participants personnalisé.

Associer une activité de flux de travaux à une tâche d'approbation.

Pour associer une activité de flux de travaux à une tâche d'approbation de flux de travaux, vous définissez une paire nom/valeur dans WorkPoint Designer.

Remarque : Si une paire nom/valeur n'est pas définie pour une activité de flux de travaux par défaut, CA IdentityMinder utilise une tâche portant un nom correspondant à la tâche d'approbation.

Pour associer une activité de flux de travaux à une tâche d'approbation.

1. Démarrer WorkPoint Designer.
2. Cliquez sur Fichier, Ouvrir, Processus.
3. Sélectionnez un processus de flux de travaux et cliquez sur Ouvrir.
4. Cliquez avec le bouton droit sur le noeud d'activité dans le processus, puis cliquez sur Propriétés.
5. Sélectionnez Texte dans le menu déroulant Type.

6. Saisissez ce qui suit dans l'onglet Données de l'utilisateur :
   - **Nom :** TASK_TAG.
   - **Valeur :** nom de balise de tâche d'approbation.
7. Cliquez sur Ajouter.
8. Cliquez sur OK pour enregistrer vos modifications.

Création de tâches d'approbation pour les terminaux

Vous pouvez créer des tâches d'approbation pour les fenêtres de gestion des comptes. Pour les tâches qui approuvent des modifications de compte, la fenêtre d'approbation doit être spécifique à un type de terminal, de sorte que l'approbateur puisse consulter les valeurs modifiées. Pour créer une tâche d'approbation pour une tâche Créer ou Modifier, procédez comme suit :

Pour créer une tâche d'approbation pour un terminal

1. Dans la console d'utilisateur, cliquez sur Rôles et tâches, Tâches d'administration, puis Créer une tâche d'administration.
2. Sélectionnez "Créer une copie de tâche d'administration" afin de gérer des comptes sur le terminal.

   Son nom doit commencer par "créer" et indiquer le nom du type de terminal. Par exemple, Créer le compte Active Directory.
3. Apportez les modifications suivantes dans l'onglet Profil.
   - Renommez la nouvelle tâche.
   - Modifiez la balise de la tâche.
   - Remplacez l'action par Approuver un événement.
4. Apportez les modifications suivantes sous l'onglet Onglets.
   a. Supprimez tous les onglets Relation.
   b. Copiez et modifiez les fenêtres d'approbation des onglets, le cas échéant.

      Remarque : Vous risquez de rencontrer des problèmes lors de l'utilisation des fenêtres de compte dans une tâche d'approbation ; vous devrez peut-être apporter des modifications à la fenêtre de compte par défaut de sorte que ces fenêtres soient opérationnelles dans une tâche d'approbation.
5. Cliquez sur Soumettre.

Outils de résolution de participants : méthode Workpoint

Pour indiquer des participants à l'aide de la méthode WorkPoint, définissez les propriétés suivantes de l'activité dans WorkPoint Designer.

- Le nom du script CA IdentityMinder prédéfini qui active la communication entre CA IdentityMinder et le serveur de flux de travaux. Le script émet une demande à CA IdentityMinder pour des participants à l'activité et fournit cette liste au serveur de flux de travaux.
- Références à un ou plusieurs outils de résolution de participants.

Types d'outils de résolution de participants

Plutôt que de saisir une liste spécifique de participants dans les propriétés de l'activité de flux de travaux, les participants sont référencés avec un nom arbitraire qui est mappé vers un *outil de résolution de participants*.

Pour le modèle de processus prédéfini, il existe quatre types d'outils de résolution de participants :

Outil de résolution de participants de rôle

Spécifie que les participants sont membres d'un rôle spécifique.

Outil de résolution de participants de groupe

Spécifie que les participants sont membres d'un groupe spécifique.

Outil de résolution de participants personnalisé

Spécifie que les participants sont déterminés selon un outil de résolution de participants personnalisé.

Outil de résolution de participants de filtre

Spécifie que les participants sont sélectionnés par le biais d'un filtre de recherche.

Outils de résolution de participants de rôle

A l'aide des outils de résolution de participants de type rôle, CA IdentityMinder extrait tous les membres de ce rôle et les renvoie en tant que participants.

Si aucun type d'outil de résolution n'est spécifié dans le paramètres UserData de la boîte de dialogue Activité, l'outil de résolution de type rôle est utilisé par défaut.

Si vous ne spécifiez aucun outil de résolution de participants dans l'onglet Données de l'utilisateur de la boîte de dialogue Propriétés de l'activité de WorkPoint, CA IdentityMinder recherche par défaut tous les rôles disponibles contenant cette tâche d'approbation et renvoie ces membres de rôle en tant que participants.

Pour configurer des outils de résolution de participants de type rôle :

1. Démarrer WorkPoint Designer.
2. Cliquez sur Fichier, Ouvrir, Processus.
3. Sélectionnez un processus de flux de travaux et cliquez sur Ouvrir.
4. Cliquez avec le bouton droit sur le noeud d'activité dans le processus, puis cliquez sur Propriétés.
5. Sélectionnez Texte dans le menu déroulant Type.
6. Saisissez ce qui suit dans l'onglet Données de l'utilisateur :
   - **Nom :** APPROVER_ROLE_NAME
   - **Valeur :** nom d'un rôle CA IdentityMinder (par exemple, gestionnaire de la sécurité)
7. Cliquez sur Ajouter.

   Remarque : Ce rôle n'a pas besoin de contenir de tâches d'approbation.
8. Sélectionnez Texte dans le menu déroulant Type.
9. Dans l'onglet Données de l'utilisateur, saisissez la paire suivante de nom/valeur (facultatif) :

   Valeur : APPROVERS_REQUIRED

   Valeur : YES.
10. Cliquez sur Ajouter.

    Remarque : Le paramètre d'approbation par défaut est APPROVERS_REQUIRED=NO. Dans ce cas, une activité est approuvée automatiquement si aucun participant n'est trouvé.

    Si APPROVERS_REQUIRED=YES et CA IdentityMinder ne trouvent aucun participant, l'activité ne peut pas se terminer correctement.
11. Cliquez sur OK pour enregistrer vos modifications.

Outils de résolution de participants de groupe

A l'aide des outils de résolution de participants de type groupe, CA IdentityMinder extrait tous les membres de ce groupe et les renvoie en tant que participants.

Pour configurer des outils de résolution de participants de type groupe :

1. Démarrer WorkPoint Designer.
2. Cliquez sur Fichier, Ouvrir, Processus.
3. Sélectionnez un processus de flux de travaux et cliquez sur Ouvrir.
4. Cliquez avec le bouton droit sur le noeud d'activité dans le processus, puis cliquez sur Propriétés.

5. Sélectionnez Texte dans le menu déroulant Type.
6. Saisissez ce qui suit dans l'onglet Données de l'utilisateur :
   - **Nom :** APPROVER_GROUP_UNIQUENAME
   - **Valeur** : nom d'un groupe CA IdentityMinder
7. Cliquez sur Ajouter.
8. Sélectionnez Texte dans le menu déroulant Type.
9. Dans l'onglet Données de l'utilisateur, saisissez la paire suivante de nom/valeur (facultatif) :
   - **Nom :** APPROVERS_REQUIRED
   - **Valeur :** YES.
10. Cliquez sur Ajouter.

    Remarque : Le paramètre d'approbation par défaut est APPROVERS_REQUIRED=NO. Dans ce cas, une activité est approuvée automatiquement si aucun participant n'est trouvé.

    Si APPROVERS_REQUIRED=YES et CA IdentityMinder ne trouvent aucun participant, l'activité ne peut pas se terminer correctement.
11. Cliquez sur OK pour enregistrer vos modifications.

Outils de résolution de participants personnalisé

L'outil de résolution de participants personnalisé est un objet Java qui détermine les participants à l'activité de flux de travaux et renvoie une liste à CA IdentityMinder, qui la transmet au moteur de flux de travaux. En général, vous écrivez uniquement un outil de résolution personnalisé si les stratégies de participant standard ne peuvent pas fournir la liste des participants requis pour une activité.

Remarque : Vous pouvez créer un outil de résolution personnalisé au moyen de l'outil de résolution de participants API. Pour plus d’informations, reportez-vous au *manuel de programmation pour Java.*

Pour configurer un outil de résolution personnalisé

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur.

   `http://hostname/iam/immanage`

   hostname

   Définit le nom de domaine complet du serveur sur lequel CA IdentityMinder est installé. Par exemple, monserveur.masociété.com:port.
2. Cliquez sur Environnements, puis sélectionnez le nom de l'environnement CA IdentityMinder approprié.

3. Cliquez sur Paramètres avancés, Outils de résolution de participants de flux de travaux.
4. Dans l'écran d'outil de résolution de participants de flux de travaux, cliquez sur Nouveau et saisissez :

   Nom

   Spécifie le nom de l'outil de résolution de participants personnalisé, par exemple, APPROVER_CUSTOMRESOLVER_NAME

   Description

   Décrit l'outil de résolution de participants personnalisé.

   Classe

   Spécifie le nom de la classe Java, par exemple, com.netegrity.samples.GroupFinder

5. Cliquez sur Enregistrer.
6. Démarrer WorkPoint Designer.
7. Cliquez sur Fichier, Ouvrir, Processus.
8. Sélectionnez un processus de flux de travaux et cliquez sur Ouvrir.
9. Cliquez avec le bouton droit sur le noeud d'activité dans le processus, puis cliquez sur Propriétés.
10. Sélectionnez Texte dans le menu déroulant Type.
11. Saisissez ce qui suit dans l'onglet Données de l'utilisateur :

    Nom

    Spécifie le nom de l'outil de résolution de participants personnalisé. Celui-ci doit correspondre au nom que vous avez saisi dans la fenêtre Outil de résolution de participants personnalisé dans la console de gestion CA IdentityMinder. Par exemple :

    APPROVER_CUSTOMRESOLVER_NAME

    Valeur

    Spécifie un nom unique pour l'outil de résolution de participants personnalisé. Par exemple : GroupFinder.

12. Cliquez sur Ajouter.

    Remarque : Le paramètre d'approbation par défaut est APPROVERS_REQUIRED=NO. Dans ce cas, une activité est approuvée automatiquement si aucun participant n'est trouvé.

    Si APPROVERS_REQUIRED=YES et CA IdentityMinder ne trouvent aucun participant, l'activité ne peut pas se terminer correctement.

13. Cliquez sur OK pour enregistrer vos modifications.

Filtre Outils de résolution de participants

Un outil de résolution de participants de type filtre active la recherche d'utilisateurs ou de groupes correspondant aux critères du filtre. Vous indiquez un filtre de recherche dans WorkPoint Designer et CA IdentityMinder renvoie des approbateurs pour l'activité de flux de travaux correspondante.

Vous créez un filtre d'outil de résolution de participants dans l'onglet Données de l'utilisateur de la boîte de dialogue Propriétés de l'activité de Workpoint.

Syntaxe du filtre d'outils de résolution de participants

Les trois attributs obligatoires suivants forment un filtre de recherche.

- Attribut de l'approbateur (par exemple, titre)
- Opérateur de l'attribut de l'approbateur (par exemple, égal(e) à
- Valeur de l'attribut de l'approbateur (par exemple, responsable)

Les attributs du filtre de recherche requis se combinent dans l'ordre suivant :

attribut opérateur valeur

Par exemple :

titre est égal à responsable ou *département contient paie*

Attributs requis de filtre d'outil de résolution de participants

Les attributs suivants sont *obligatoires* pour le filtre de l'outil de résolution de participants.

Remarque : Pour chaque filtre, n est un nombre entier positif indiquant le nombre de filtres de recherche. La valeur par défaut est 1.

APPROVER_FILTER_n_ATTRIBUTE

Spécifie l'attribut de l'approbateur. Par exemple, Titre, Département, ID de l'utilisateur. Les chaînes de noms d'attributs d'approbateurs doivent correspondre à celles de l'utilisateur CA IdentityMinder.

APPROVER_FILTER_n_OP

Spécifie l'opérateur associé à l'attribut de l'approbateur. Par exemple, égal, non_égal ou contient. (Les mots clés de l'opération ne sont pas sensibles à la casse).

Les entrées suivantes sont valides pour ce filtre.

- EQUALS
- STARTSWITH

- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

Spécifie la valeur associée à l'approbateur. Par exemple, responsable, paie, ingénierie

Attributs facultatifs de filtre d'outil de résolution de participants

Les attributs suivants sont *facultatifs* pour le filtre de l'outil de résolution de participants.

APPROVER_OBJECTTYPE

USER ou GROUP (non sensible à la casse)

Par défaut, USER.

APPROVER_ORG_UNIQUENAME

Un nom unique pour une organisation de l'approbateur. (Les chaînes de noms des organisations doivent correspondre aux chaînes de noms des organisations d'Identity Manager.)

La valeur par défaut est root.

APPROVER_ORG_AND_LOWER

L'organisation ou les sous-organisations de l'approbateur :

- 0 signifie recherche dans l'organisation de l'approbateur.
- 1 signifie recherche dans la sous-organisation de l'approbateur.

La valeur par défaut est 1.

APPROVER_FILTER_NO

Le nombre de filtres de recherche que vous êtes en train d'utiliser. Si vous avez deux filtres, ce chiffre serait 2.

La valeur par défaut est 1.

Remarque : Ce filtre est obligatoire si plusieurs filtres existent.

APPROVER_FILTER_n_CONJ_TYPE

Vous pouvez combiner des filtres de recherche en utilisant des types de conjonction comme OU ou ET.

Remarque : Les filtres séparés par la conjonction OU sont prioritaires par rapport à ceux séparés par ET.

Par exemple, vous pouvez spécifier le type de conjonction ET si vous recherchez "titre égale à responsable" ET "département égale développement".

Remarque : n est un nombre entier positif supérieur à 1 indiquant le nombre de filtres de recherche.

Ajouter un filtre d'outil de résolution de participants

Pour ajouter des filtres à l'outil de résolution de participants :

1. Démarrer WorkPoint Designer.
2. Cliquez sur Fichier, Ouvrir, Processus.
3. Sélectionnez un processus de flux de travaux et cliquez sur Ouvrir.
4. Cliquez avec le bouton droit sur le noeud d'activité dans le processus, puis cliquez sur Propriétés.
5. Sélectionnez Texte dans le menu déroulant Type.
6. Saisissez ce qui suit dans l'onglet Données de l'utilisateur :
   - **Nom :** APPROVER_FILTER_1_ATTRIBUTE
   - **Valeur :** un identifiant de rôle unique (par exemple, titre).
7. Cliquez sur Ajouter.
8. Répétez les étapes 6 et 7 pour chaque attribut dans le filtre de recherche.

   Remarque : Le paramètre d'approbation par défaut est APPROVERS_REQUIRED=NO. Dans ce cas, une activité est approuvée automatiquement si aucun participant n'est trouvé.

   Si APPROVERS_REQUIRED=YES et CA IdentityMinder ne trouvent aucun participant, l'activité ne peut pas se terminer correctement.
9. Cliquez sur OK pour enregistrer vos modifications.

Exemple : Filtre Outil de résolution de participants

Le magasin d'utilisateurs dans le tableau suivant contient quatre utilisateurs : Holly, Sarah, John et Dave avec des attributs d'ID de l'utilisateur, titre de job et département.

Utilisateur	ID	Titre	Service
Holly	admin1	adminsys	administration

Utilisateur	ID	Titre	Service
Sarah	test1	adminsys	développement
John	admin2	gestionnaire	développement
Dave	admin3	adminsys	comptabilité

CA IdentityMinder applique les trois filtres définis dans le tableau suivant en fonction du magasin d'utilisateurs précédent.

Nom	Valeur
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	est égal à
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	ET
APPROVER_FILTER_2_ATTRIBUTE	département
APPROVER_FILTER_2_OP	est égal à
APPROVER_FILTER_2_VALUE	administration
APPROVER_FILTER_3_CONJ_TYPE	OU
APPROVER_FILTER_3_ATTRIBUTE	titre
APPROVER_FILTER_3_OP	est égal à
APPROVER_FILTER_3_VALUE	adminsys

CA IdentityMinder applique les filtres dans l'ordre ci-dessous.

1. Evalue le deuxième et le troisième filtres connectés par la conjonction OU.

   "département égale à administration" OU "titre égale à adminsys"

   Ces filtres excluent John et renvoient Holly, Sarah et Dave.

2. Evalue le premier et le deuxième filtres connectés par la conjonction ET, où * correspond à un caractère générique.

   "uid égale admin*" ET "département égale administration"

   Ces filtres excluent Sarah et renvoient Holly et Dave.

Les utilisateurs finaux renvoyés par le magasin d'utilisateurs sont Holly et Dave.

Ordre de priorité des outils de résolution de participants

Si vous ne spécifiez aucun outil de résolution de participants, Identity Manager identifie par défaut tous les rôles disponibles contenant la tâche d'approbation et renvoie ces membres de rôle en tant que participants.

Si vous indiquez plus d'un outil de résolution de participants, Identity Manager les évalue selon cet ordre de priorité :

1. Personnalisé
2. Rôle
3. Filtre
4. Groupe

Identity Manager identifie et applique le premier outil de résolution dans cet ordre de priorité et ignore tout outil de résolution ultérieur restant.

Vous ne devriez avoir qu'un outil de résolution à la fois. De même, assurez-vous que l'outil de résolution est bien configuré afin qu'Identity Manager identifie correctement les participants.

Spécifier le script de ressource de flux de travaux

Identity Manager est fourni avec un script, appelé IM Approvers, qui transmet des informations entre Identity Manager et le serveur de flux de travaux.

Quand une liste de participants est requise pour une activité de flux de travaux, le script transmet à Identity Manager le nom de l'activité, l'identifiant du participant fourni dans l'onglet Données de l'utilisateur de la boîte de dialogue Propriétés de l'activité de WorkPoint et tout autre information fournie dans l'onglet Données de l'utilisateur. Identity Manager recherche des participants et transmet la liste en retour au script. Le script fournit alors la liste au serveur de flux de travaux.

Lorsque vous avez une nouvelle définition de processus de flux de travaux et que l'activité du processus de flux de travaux est une tâche d'approbation de flux de travaux d'Identity Manager, le script IM Approvers doit être indiqué dans l'onglet Ressources de la boîte de dialogue Propriétés de l'activité de WorkPoint.

Pour indiquer le script IM Approvers dans WorkPoint Designer

1. Dans l'onglet Ressources, cliquez sur Sélectionner.
2. Dans la boîte de dialogue Sélectionner les ressources, sélectionnez Règle dans la liste déroulante. Cette action permet de lister les règles (scripts) que vous pouvez associer à l'activité.

3. Sélectionnez le nom du script IM Approvers, puis cliquez sur Ajouter.
4. Cliquez sur OK, puis sur Appliquer dans la boîte de dialogue Propriétés de l'activité.

Remarque : Ne modifiez pas le script IM Approvers.

Spécifier les participants pour les tâches Certifier un utilisateur

Les tâches Certifier un utilisateur génèrent un événement CertifyRoleEvent. Cet événement peut être soumis à une approbation du flux de travaux par l'intermédiaire du processus prédéfini CertifyRoleApproveProcess.

Identity Manager inclut aussi l'outil de résolution de participants prédéfini CertifyRoleParticipantResolver, qui est présent dans votre environnement par défaut. Les participants pour des activités dans CertifyRoleApprovalProcess sont spécifiés avec CertifyRoleParticipantResolver.

Pour fournir des informations de configuration des participants

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur.

   `http://hostname/iam/immanage`

   hostname

   Définit le nom de domaine complet du serveur sur lequel CA IdentityMinder est installé. Par exemple, monserveur.masociété.com:port.

2. Cliquez sur Environnements, puis sélectionnez le nom de l'environnement CA IdentityMinder approprié.
3. Cliquez sur Paramètres avancés puis sur Divers.
4. Définissez des paires nom/valeur qui indiquent les approbateurs pour chaque rôle à certifier :
   - Dans le champ Propriété, utilisez le format : *role-type.role-name*

     role-type doit être l'un de ces rôles : administrateur, accès, provisionnement.

     role-name est le nom d'un rôle existant.

     Le role-name et le role-type doivent être séparés par un point (.).
   - Dans le champ Valeur, spécifiez l'ID des approbateurs et séparez les ID avec un point-virgule (;).

Dans l'exemple suivant, la certification des utilisateurs peut être approuvée pour les rôles suivants et les participants suivants :

- jsmith01 et ajones19 peuvent approuver la certification pour le rôle de gestionnaire d'utilisateurs ;
- plewis12 est le seul approbateur pour le rôle de gestionnaire de système ;
- rtrevor8 et pkitt3 peuvent approuver la certification pour le rôle Mon accès.

Propriété	**Valeur**
admin.User Manager	jsmith01;ajones19
admin.System Manager	plewis12
access.My Access Role	rtrevor8;pkitt3

Remarque : Tous les rôles non spécifiés n'auront pas d'approbateurs pour CertifyRoleEvent.

Processus dans WorkPoint Designer

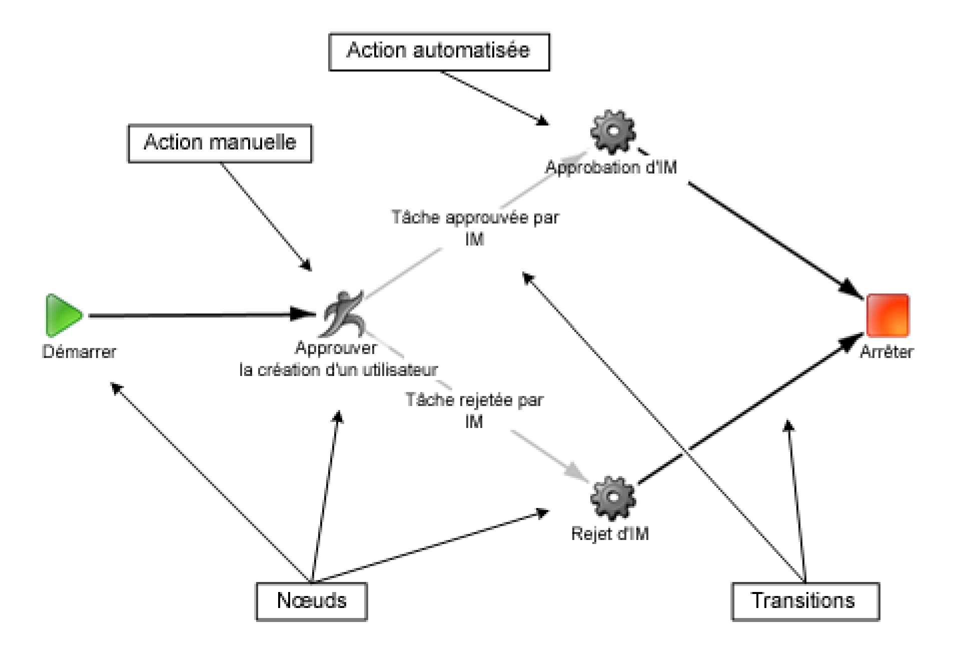
Dans WorkPoint Designer, vous pouvez personnaliser les processus de flux de travaux et les activités par défaut qui sont fournies avec Identity Manager et vous pouvez en créer de nouvelles.

Ce document présente des informations sur le flux de travaux de WorkPoint, qui est spécifique d'Identity Manager. Pour plus d'informations, reportez-vous à la documentation de WorkPoint Designer.

Remarque : Lors de la création d'un processus de flux de travaux, n'oubliez pas de faire une copie du processus existant d'Identity Manager, puis modifiez le nouveau processus selon vos besoins. Un processus de flux de travaux créé ainsi inclut des éléments par défaut spécifiques d'Identity Manager et des noeuds comme des scripts de transition et des activités automatisées.

Diagramme de processus de flux de travaux

Le diagramme suivant montre un processus de flux de travaux typique avec l'ensemble minimum de composants pour un processus contrôlant une tâche d'Identity Manager task. Le diagramme illustre le processus prédéfini CreateUserApproveProcess, qui contrôle l'exécution d'une tâche Créer un utilisateur.



Composants de processus de WorkPoint

Le processus de flux de travaux comprend les noeuds et transitions suivantes :

Démarrer

Chaque flux de travaux commence avec ce noeud.

Arrêter

Chaque flux de travaux termine avec ce noeud.

Activité manuelle

Une activité manuelle nécessite l'approbation ou le rejet d'une tâche d'Identity Manager par un participant et doit porter le même nom qu'une tâche d'approbation de flux de travaux d'Identity Manager.

Un processus de flux de travaux contrôlant une tâche d'Identity Manager doit inclure au moins une activité manuelle nécessitant l'approbation de cette tâche.

Activité automatisée

Un ou deux scripts sont affectés à une activité automatisée :

- Notify IM Approve : informe Identity Manager qu'il doit exécuter la tâche d'Identity Manager sous le contrôle d'un flux de travaux ;
- Notify IM Reject : informe Identity Manager qu'il doit annuler l'exécution de la tâche d'Identity Manager.

En général, le script Notify IM Approve est activé si toutes les activités manuelles sont approuvées et le script Notify IM Reject est activé si une activité manuelle est rejetée.

Transition inconditionnelle

Une transition inconditionnelle est un chemin entre un noeud dans le processus de flux de travaux et un autre noeud et il n'est pas associé à un script de condition.

Transition conditionnelle

Une transition conditionnelle représente un autre chemin entre un noeud dans le processus de flux de travaux et un autre noeud et il est associé à un script de condition.

Un script de condition détermine si la transition se produit en évaluant le résultat de l'activité associée. Si le script renvoie vrai, la transition s'est effectuée et le processus avance vers le prochain noeud indiqué.

Il est possible que deux scripts de condition ou plus renvoient vrai. Il est alors possible d'effectuer une activité en parallèle, étant donné que chaque script est associé à une transition différente.

Remarque : Vous pouvez utiliser des scripts personnalisés dans des transitions conditionnelles. Vous trouverez des instructions dans le *manuel de programmation pour Java.*

Propriétés d'activité manuelle

Les paramètres des propriétés spécifiques d'Identity Manager sont listées dans le tableau suivant. Ces paramètres sont définis dans les onglets indiqués de la boîte de dialogue Propriétés de l'activité de WorkPoint Designer.

Onglet Propriétés	Descriptions des propriétés
Ressources	IM Approvers : indiqué dans la liste Inclure. Ce script transmet des informations entre Identity Manager et le serveur de flux de travaux.
Agents	Nobody Auto Complete : indiqué dans la liste Asynchrone et associé à l'état Disponible. Ce script détermine si une activité doit être considérée comme approuvée si aucun participant à l'activité existe.

Onglet Propriétés	Descriptions des propriétés
Données de l'utilisateur	Définit des paires nom/valeur qu'Identity Manager utilise pour extraire les participants de l'activité. Vous pouvez éventuellement définir des données à transmettre à un outil de résolution de participants personnalisé.

Propriétés d'une transition conditionnelle

Les scripts suivants par défaut apparaissent dans l'onglet Condition de la boîte de dialogue Propriété d'une transition :

IM WorkItem Approved

Renvoie vrai si l'activité associée est approuvée. Le processus de flux de travaux fonctionne vers le prochain noeud indiqué par la transition.

IM WorkItem Rejected

Renvoie vrai si l'activité associée est rejetée. Le processus de flux de travaux fonctionne vers le prochain noeud indiqué par la transition.

Instances et jobs et de processus

Un *processus de flux de travaux* définit les étapes à suivre avant qu'Identity Manager puisse terminer une tâche particulière. Un *job* est une instance d'exécution d'un processus de flux de travaux.

Par exemple, le processus de flux de travaux par défaut CreateUserApproveProcess définit les étapes qui doivent se produire pour qu'un nouvel utilisateur soit approuvé. Quand un nouvel utilisateur est vraiment créé dans Identity Manager et que la tâche est soumise pour approbation, une instance de job de CreateUserApproveProcess est créée dans WorkPoint Designer.

Vous pouvez ouvrir, afficher et modifier des jobs dans WorkPoint Designer à l'aide d'une interface qui ressemble beaucoup à celle utilisée pour modifier les processus de flux de travaux.

Plusieurs jobs basés sur le même processus peuvent exister simultanément.

Filtrage de jobs

WorkPoint Designer inclut un filtrage, qui vous permet de rechercher des jobs basés sur différents critères. Par exemple, vous pouvez rechercher des jobs qui :

- sont basés sur un ou plusieurs processus de flux de travaux sélectionnés ;
- ont une référence de job définie par l'utilisateur ou un ID de job unique .

- sont dans un état particulier (comme actif, terminé ou suspendu) ;
- ont été créés ou commencés pendant un intervalle de dates spécifié.

Remarque : Vous trouverez des instructions et des informations de référence sur le filtrage de job dans la documentation de WorkPoint Designer.

Etats et propriétés de jobs

Lorsque vous ouvrez un job, le diagramme du flux de travaux du job est affiché. Les noeuds et les transitions de l'activité du flux de travaux sont représentés en couleurs, ce qui indique s'ils ont été effectués.

Vous pouvez afficher et parfois modifier :

- des propriétés d'un job, y compris l'historique des participants et du job ;
- l'état du job ouvert, par exemple s'il a été terminé ;
- des propriétés des noeuds et transitions individuels dans un job.

Propriétés des activités et des tâches

Vous pouvez afficher et parfois modifier les propriétés de l'activité d'un job et les propriétés de l'activité d'un processus, y compris :

- les informations de l'état d'activité ;
- les informations d'approbation de l'activité ;
- les informations de la tâche d'approbation (appelée *tâche* dans WorkPoint Designer), par exemple :
  - si aucun participant n'a réservé la tâche (ce qui supprime la tâche de la liste des travaux d'autres approbateurs), l'état est Disponible et aucun ID de participant n'est affiché ;
  - si un participant a réservé mais n'a pas encore terminé la tâche, l'état est Ouverte et l'ID du participant et l'heure de réservation sont affichés ;
  - si la tâche a été terminée, l'état est Terminée. L'ID d'utilisateur du participant qui a approuvé ou rejeté la tâche sous le contrôle du flux de travaux est affiché, ainsi que l'heure de fin.

Les propriétés de tâches spécifiques incluent :

- le nom et l'état actuel de la tâche ;
- l'historique de l'état, y compris l'ID d'utilisateur des participants responsables des états donnés ;
- l'historique des participants de la tâche autorisée.

Remarque : Pour plus d'informations sur les propriétés de jobs, d'activités et de tâches, reportez-vous à la documentation de WorkPoint Designer.

Réalisation d'activités de flux de travaux

Dans un processus de flux de travaux, une activité manuelle est réalisée par une personne désignée par un participant à l'activité qui approuve ou rejette un événement associé à une tâche d'approbation. Les participants réalisent cette activité dans Identity Manager.

Les opérations suivantes ont lieu quand une activité associée à une tâche approuvée d'Identity Manager est réalisée :

1. Identity Manager envoie une notification aux participants.
2. Un participant approuve ou rejette la tâche.
3. Le serveur de flux de travaux termine l'activité.

Trouver et envoyer une notification aux participants

Quand une activité associée à une tâche d'approbation d'Identity Manager commence, le serveur de flux de travaux transmet les informations concernant les participants à l'activité à Identity Manager. Ce informations sont définies dans les propriétés de l'activité. Identity Manager utilise ces informations pour extraire les participants à l'activité et les prévenir qu'une tâche d'approbation est en attente.

Après avoir identifié les participants, Identity Manager ajoute une nouvelle tâche (la tâche d'approbation) dans la liste de travail de chaque participant. Identity Manager envoie également éventuellement un courriel de notification sur la nouvelle tâche à chaque participant.

Remarque : Si la propriété de l'activité APPROVERS_REQUIRED est définie sur faux et qu'aucun participant n'a été trouvé, la tâche est considérée comme approuvée par défaut.

Remarque : Un cercle dans la colonne Etat indique que la tâche d'approbation est disponible si un participant veut la prendre en charge. Une coche indique que le propriétaire de la liste de travail a accepté la tâche d'approbation mais ne l'a pas encore terminée.

Accepter et réaliser la tâche d'approbation

Une fois les participants trouvés, l'activité ne peut pas être terminée tant qu'un participant n'a pas accepté la tâche d'approbation et accepté ou rejeté la tâche sous le contrôle du flux de travaux.

Un participant accepte une tâche d'approbation en cliquant sur le nom de la tâche dans la console d'activité du flux de travaux et en cliquant ensuite sur Réserver un élément. Le fait de réserver un élément le supprime de la liste de travail des autres approbateurs.

Quand un participant a accepté une tâche d'approbation, il s'engage à prendre la décision d'approbation ou de rejet de la tâche sous le contrôle du flux de travaux. Ensuite, étant donné que plusieurs participants ne peuvent pas accepter la même tâche d'approbation, cette dernière est supprimée de la liste de travail des autres participants.

Une fois qu'un participant a accepté une tâche d'approbation, une fenêtre d'approbation apparaît dans lequel le participant peut choisir l'une de ces actions :

- approuver ou rejeter immédiatement la tâche sous le contrôle du flux de travaux ;
- libérer la tâche d'approbation afin de la rendre disponible pour les autres participants ;
- fermer la boîte de dialogue et terminer l'activité plus tard. Pour rouvrir la boîte de dialogue Approuver la création d'un utilisateur qui figure au-dessus, le participant clique sur le nom de la tâche d'approbation dans sa liste de travail.

De plus, le participant peut mettre à jour un ou plusieurs champs modifiables, le cas échéant, sur l'écran d'approbation. Vous pouvez rendre des champs modifiables sur cette fenêtre lors de la création de la tâche.

Une fois que le participant a approuvé ou rejeté la tâche sous le contrôle du flux de travaux, l'activité est terminée et le processus de flux de travaux peut continuer sur le chemin déterminé par le résultat de l'activité, qui est décrit dans la prochaine section.

Le serveur de flux de travaux termine l'activité.

Une activité manuelle apparaît dans la fenêtre de Designer avec deux transitions conditionnelles ou plus y menant.

Chaque transition conditionnelle est associée à un script. Quand un participant termine l'activité, les scripts évaluent le résultat de l'activité. Le résultat de ces évaluations détermine la direction du flux de processus.

L'illustration suivante montre l'activité Approuver la création d'un utilisateur dans Designer et la tâche d'approbation correspondante portant le même nom dans Identity Manager.

Quand le participant à l'activité (ou l'approbateur) clique sur le bouton Approuver ou Rejeter dans Identity Manager :

1. L'activité Approuver la création d'un utilisateur dans l'instance de job de processus prend fin. Les scripts associés aux transitions conditionnelles évaluent le résultat de l'activité.

2. L'instance de job continue, selon la transition conditionnelle qui est évaluée comme vraie :

   - Si l'activité est approuvée, le script IM WorkItem Approved renvoie vrai. Le flux de travaux mène la transition IM WorkItem Approved vers le prochain noeud. Cette activité automatisée, IM Approve, envoie une notification à Identity Manager pour qu'il exécute la tâche Créer un utilisateur.
   - Si l'activité est rejetée, le script IM WorkItem Rejected renvoie vrai. Le flux de travaux mène la transition IM WorkItem Rejected vers le prochain noeud du flux de travaux. Cette activité automatisée, IM Reject, envoie une notification à Identity Manager pour qu'il annule la tâche Créer un utilisateur.

Affichage du job Workpoint

Vous pouvez afficher l'état d'exécution des jobs Workpoint dans la console d'utilisateur à partir des éléments ci-après.

- Tâches d'approbation
- Afficher les tâches soumises

Dans les nouveaux environnements, toutes les tâches d'approbation comprennent l'onglet Afficher le job par défaut. Seuls les événements créés dans cette version prennent en charge l'affichage des images de job pour toutes les définitions de processus invoquées pour l'événement ou la tâche sélectionné(e) dans Afficher les tâches soumises. Les événements créés dans des versions antérieures ne prennent pas en charge la fonction Affichage du job contenu dans le flux de travaux des événements.

Ajout de l'onglet Afficher le job aux onglets Approbation existants

Pour les tâches d'approbation, vous devez ajouter le nouvel onglet Afficher le job à toutes les tâches existantes afin d'afficher l'image du job pour cette tâche.

Remarque : Les nouveaux environnements incluent cet onglet pour toutes les tâches d'approbation.

Pour ajouter l'onglet Afficher le job à une tâche existante :

1. A partir de Tâches d'administration et du rôle Catégorie, exécutez ModifyAdminTask en sélectionnant Tâche d'administration, Modifier la tâche d'administration
2. Cliquez sur Rechercher, sélectionnez une tâche d'approbation (par exemple, Approuver la création d'un utilisateur), puis cliquez sur Sélectionner.

   La boîte de dialogue Approuver la création d'un utilisateur de Modifier la tâche d'administration apparaît.
3. Cliquez sur l'onglet Onglets. Dans le menu déroulant, sélectionnez Afficher le job (JobView), puis cliquez sur Soumettre.

   L'onglet Afficher le job a été ajouté à la tâche d'approbation.

   Répétez cette procédure pour toutes les tâches d'approbation existantes.

Configuration de l'onglet Afficher le job

Configurez cet onglet avec les éléments ci-dessous.

Nom

Nom que vous affectez à l'onglet.

Balise

Identifiant unique pour l'onglet au sein de la tâche. Elle doit commencer par une lettre ou un caractère de soulignement et contenir uniquement des lettres, des chiffres ou des caractères de soulignement. La balise est principalement utilisée pour définir des valeurs de données via des documents XML ou des paramètres HTTP.

Masquer l'onglet

Empêche l'onglet d'être visible dans la tâche. Cette option est utile pour les applications qui doivent masquer l'onglet, mais qui ont toujours accès aux attributs de cet onglet.

IM--Affichage du job

Cet onglet affiche l'image du job pour la tâche spécifiée.

Affichage de l'onglet Afficher le job sur une tâche d'approbation.

Pour afficher l'onglet Afficher le job sur une tâche d'approbation, procédez comme suit :

Pour afficher l'onglet Afficher le job :

1. Dans la boîte de dialogue Liste de travail, sélectionnez la tâche d'approbation à afficher.
2. Cliquez sur l'onglet Afficher le job pour afficher le statut d'exécution de la tâche.

   Vous pouvez ensuite approuver, rejeter, réserver ou fermer l'onglet.

Vous pouvez également cliquer sur l'onglet Accueil et Afficher ma liste de travail pour accéder à la boîte de dialogue Liste de travail.

Affichage du job contenu dans un flux de travaux de niveau événement

Pour afficher un job contenu dans un flux de travaux de niveau événement dans Afficher les tâches soumises, procédez comme suit.

Pour afficher un job contenu dans le flux de travaux :

1. Dans l'onglet Systèmes, sélectionnez Afficher les tâches soumises, entrez vos critères de recherche, puis sélectionnez Rechercher.
2. Sélectionnez l'événement, puis cliquez sur le crayon pour afficher les détails correspondants.
3. Sous Affichage du job contenu dans le flux de travaux de niveau événement, sélectionnez le processus, puis cliquez sur le crayon pour afficher l'image du job pour cet événement.

Affichage du job contenu dans un flux de travaux de niveau tâche

Pour afficher un job contenu dans un flux de travaux de niveau tâche dans Afficher les tâches soumises, procédez comme suit.

Pour afficher un job contenu dans le flux de travaux :

1. Dans l'onglet Systèmes, sélectionnez Afficher les tâches soumises, entrez vos critères de recherche, puis sélectionnez Rechercher.
2. Sélectionnez la tâche, puis cliquez sur le crayon pour afficher les détails correspondants.

Sous Affichage du job contenu dans le flux de travaux de niveau tâche, sélectionnez le processus, puis cliquez sur le crayon pour afficher l'image du job pour cette tâche.

Flux de travaux utilisant des stratégies

Le flux de travaux utilisant des stratégies permet de placer un événement ou une tâche d'administration sous le contrôle du flux de travaux en fonction de l'évaluation d'une règle. De cette manière, l'événement ou la tâche d'administration ne lance pas systématiquement un processus de flux de travaux : au lieu de cela, le processus de flux de travaux est exécuté et génère une tâche uniquement si une règle associée à l'événement ou à la tâche d'administration est respectée.

Une *règle d'approbation* est une condition qui détermine s'il est nécessaire de démarrer un processus de flux de travaux. S'il est démarré, le processus de flux de travaux place l'événement ou la tâche d'administration sous le contrôle du flux de travaux en ajoutant une tâche à la liste de travail d'un approbateur.

Une *stratégie d'approbation* désigne la combinaison de la règle d'approbation, du processus de flux de travaux et des informations associées.

Par exemple, lorsque vous créez un groupe, vous pouvez définir une stratégie d'approbation qui place l'événement CreateGroupEvent sous le contrôle du flux de travaux et crée une tâche uniquement si le nouveau groupe fait partie d'une organisation parente désignée. Dans le cas contraire, le processus de flux de travaux n'est pas exécuté et aucune tâche n'est créée.

Comme pour une tâche d'administration, vous pouvez définir une stratégie d'approbation qui place la tâche CreateGroupTask sous le contrôle du flux de travaux et crée une tâche uniquement si le nom du nouveau groupe commence par Ventes. Dans le cas contraire, le processus de flux de travaux n'est pas exécuté et aucune tâche n'est créée.

Vous pouvez créer une règle de stratégie qui est toujours évaluée ou uniquement lorsqu'un attribut spécifié d'un objet géré est modifié, par exemple la valeur du salaire d'un employé.

Informations complémentaires :

Ordre de stratégies (page 476)
Evaluation des règles (page 474)
Flux de travaux au niveau événement (page 429)
Flux de travaux de niveau tâche (page 426)

Processus de flux de travaux par défaut

Tous les modèles de flux de travaux par défaut et prédéfinis prennent en charge les règles de flux de travaux, comme suit.

- **Modèles de processus** : vous permettent de configurer les approbateurs (ou les outils de résolution de participants) dans la console d'utilisateur.
- **Processus de flux de travail prédéfinis** : nécessitent de configurer les outils de résolution de participants dans WorkPoint Designer.

Vous pouvez également créer des processus de flux de travaux personnalisés à utiliser avec les règles de flux de travaux.

Informations complémentaires :

Processus WorkPoint (page 444)

Objets des règles

Un administrateur CA IdentityMinder peut créer des stratégies d'approbation pour un événement ou une tâche d'administration sur la base des objets suivants. Voici les objets pour un événement s'ils s'appliquent à un événement donné et sont présents lors de l'exécution de l'événement :

- **Auteur de la tâche** : administrateur CA IdentityMinder qui exécute la tâche.
- **Objet principal de l'événement** : objet principal associé à l'événement.
- **Objet secondaire de l'événement** : objet secondaire associé à l'événement relatif à l'objet principal.

Les objets pour une tâche d'administration sont les suivants.

- **Objet principal de la tâche** : objet principal associé à la tâche.
- **Auteur de la tâche** : administrateur Identity Manager qui exécute la tâche.
- **Violations de stratégie d'identité** : concernant les violations de stratégie d'identité, les règles se basent sur le nom de la stratégie d'identité à l'origine de la violation, par exemple, Nom de la stratégie EGAL A TitlePolicy. Le message de violation s'affiche sous l'onglet Détails de la tâche de la fenêtre Approbation, qui est identique aux détails de la tâche de la fenêtre Afficher les tâches soumises. Le message de violation de séparation des fonctions apparaît sous une nouvelle section intitulée Violations de la stratégie d'identité. Un approbateur peut consulter ces messages et décider d'approuver ou de rejeter la tâche.

Evaluation des règles

Les règles de stratégie associées à un événement peuvent être évaluées de deux manières.

- Toujours

  Une stratégie ayant comme type d'évaluation Always (Toujours) est invoquée si la stratégie est évaluée comme True, que les attributs qu'elle contient aient été modifiés ou non. Dans la fenêtre d'approbation d'une tâche générée en raison d'une stratégie dont le type d'évaluation est Always, un approbateur peut modifier tous les attributs modifiables.

  Remarque : Si l'approbateur clique sur le bouton Rejeter, l'événement est rejeté tel qu'il était auparavant.

- Uniquement si un attribut spécifié dans la condition d'approbation est modifié

  Une stratégie dont le type d'évaluation est OnChange (Lors de la modification) n'est invoquée que si la stratégie est évaluée comme True et qu'au moins un de ses attributs a été modifié. Dans la fenêtre d'approbation d'une tâche générée en raison d'une stratégie dont le type d'évaluation est Onchange, l'approbateur peut uniquement modifier la valeur des attributs contenus dans cette stratégie, si ces attributs présentent une autorisation lecture-écriture pour cette fenêtre d'approbation. Tous les autres attributs qui existent dans cette fenêtre sont en lecture seule.

  Remarque : Si l'approbateur clique sur le bouton Rejeter, seuls les changements apportés aux attributs contenus dans la stratégie d'approbation sont rejetés et la stratégie d'approbation suivante est évaluée.

  Cette option ne s'applique qu'à l'objet principal de l'événement ou de la tâche.

Prenons l'exemple des stratégies suivantes associées à l'événement ModifyUserEvent de la tâche d'administration Modifier un utilisateur.

Stratégie	Règle	Evaluation
Stratégie 1	Utilisateur où (ID de l'utilisateur = Smith01)	Toujours
Stratégie 2	Utilisateur où (Titre = Gestionnaire)	Lorsque l'attribut Titre est modifié
Stratégie 3	Utilisateur où (Salaire >= 80000)	Lorsque l'attribut Salaire est modifié

La Stratégie 1 est évaluée à chaque fois que l'administrateur invoque la tâche Modifier un utilisateur pour l'utilisateur Smith01, quel que soit l'attribut modifié.

La Stratégie 2 est évaluée lorsque l'administrateur invoque la tâche Modifier un utilisateur pour modifier l'attribut Titre de n'importe quel objet Utilisateur. La Stratégie 2 a la valeur True si le Titre devient Gestionnaire.

La Stratégie 3 est évaluée lorsque l'administrateur invoque la tâche Modifier un utilisateur pour modifier l'attribut Salaire de n'importe quel objet Utilisateur. La Stratégie 3 a la valeur True si la modification du salaire élève ce dernier à 80 000 ou plus.

Dans cet exemple, si un administrateur utilise la tâche Modifier un utilisateur pour changer l'attribut Titre en Gestionnaire pour l'utilisateur Smith01, la Stratégie 1 et la Stratégie 2 renvoient la valeur True et leurs processus de flux de travaux respectifs sont lancés. Dans ce cas, la priorité de classement standard s'applique.

L'évaluation de règle conditionnelle permet à l'approbateur d'une tâche de modifier un attribut qui affecte une autre tâche pour le même événement alors que ce dernier est encore en attente. Ceci n'est possible que pour les stratégies d'approbation dont le type d'évaluation est Always. Dans l'exemple précédent, si un administrateur modifie un attribut pour l'utilisateur Smith01, la Stratégie 1 a la valeur True et génère une tâche. Tout en approuvant la tâche générée par la Stratégie 1, cet approbateur peut, dans la même fenêtre d'approbation, modifier l'attribut Salaire pour Smith01. Dans ce cas, la nouvelle valeur Salaire pour Smith01 détermine si la Stratégie 3 génère une tâche pour la même instance de l'événement ModifyUserEvent. Si l'approbateur attribue la valeur 90 000 au salaire, la Stratégie 3 génère une nouvelle tâche qui doit être approuvée avant l'événement. La priorité de classement standard s'applique.

Informations complémentaires :

Ordre de stratégies (page 476)
Objets des règles (page 473)

Exemple d'évaluation des règles

Prenons l'exemple des stratégies suivantes associées à l'événement ModifyUserEvent de la tâche d'administration Modifier un utilisateur :

Stratégie	Règle	Evaluation
Stratégie 1	Utilisateur où (ID de l'utilisateur = Smith01)	Always
Stratégie 2	Utilisateur où (Titre = Gestionnaire)	Lorsque l'attribut Titre est modifié
Stratégie 3	Utilisateur où (Salaire >= 80000)	Lorsque l'attribut Salaire est modifié

La Stratégie 1 est évaluée à chaque fois que l'administrateur invoque la tâche Modifier un utilisateur pour l'utilisateur Smith01, quel que soit l'attribut modifié.

La Stratégie 2 est évaluée lorsque l'administrateur invoque la tâche Modifier un utilisateur pour modifier l'attribut Titre de n'importe quel objet Utilisateur. La Stratégie 2 a la valeur True si le Titre devient Gestionnaire.

La Stratégie 3 est évaluée lorsque l'administrateur invoque la tâche Modifier un utilisateur pour modifier l'attribut Salaire de n'importe quel objet Utilisateur. La Stratégie 3 a la valeur True si la modification du salaire élève ce dernier à 80 000 ou plus.

Dans cet exemple, si un administrateur utilise la tâche Modifier un utilisateur pour changer l'attribut Titre en Gestionnaire pour l'utilisateur Smith01, la Stratégie 1 et la Stratégie 2 renvoient la valeur True et leurs processus de flux de travaux respectifs sont lancés. Dans ce cas, la priorité de classement standard s'applique.

L'évaluation de règle conditionnelle permet à l'approbateur d'une tâche de modifier un attribut qui affecte une autre tâche pour le même événement alors que ce dernier est encore en attente. Ceci n'est possible que pour les stratégies d'approbation dont le type d'évaluation est Always. Dans l'exemple précédent, si un administrateur modifie un attribut pour l'utilisateur Smith01, la Stratégie 1 a la valeur True et génère une tâche. Tout en approuvant la tâche générée par la Stratégie 1, cet approbateur peut, dans la même fenêtre d'approbation, modifier l'attribut Salaire pour Smith01. Dans ce cas, la nouvelle valeur Salaire pour Smith01 détermine si la Stratégie 3 génère une tâche pour la même instance de l'événement ModifyUserEvent. Si l'approbateur attribue la valeur 90 000 au salaire, la Stratégie 3 génère une nouvelle tâche qui doit être approuvée avant l'événement. La priorité de classement standard s'applique.

Ordre de stratégies

Toutes les stratégies d'approbation contiennent un champ Ordre de stratégies dans lequel une valeur entière positive, triée par ordre croissant, spécifie la priorité. La priorité de chaque stratégie détermine ce qui suit.

- Ordre d'évaluation des règles d'approbation
- Pour les règles respectées, l'ordre de démarrage des processus de flux de travaux.

Une stratégie disposant d'une valeur entière inférieure est associée à une priorité plus élevée et sa règle est évaluée avant une stratégie disposant d'une valeur entière supérieure. Parmi toutes les stratégies d'un événement ou d'une tâche d'administration qui sont respectées, c'est la stratégie qui dispose de la priorité la plus élevée qui lance en premier le processus de flux de travaux associé.

Exemple d'ordre de stratégie

Cet exemple illustre le fonctionnement de l'ordre des stratégies. Il suppose que les règles de stratégie sont toujours évaluées.

Si un événement dispose de plusieurs stratégies qui sont toujours évaluées, toutes les stratégies de l'événement à approuver doivent être approuvées pour que celui-ci le soit aussi. Par contre, si une seule stratégie associée à l'événement qui a ALWAYS comme type d'évaluation de stratégie est rejetée, l'événement proprement dit est également rejeté.

Remarque : Si une stratégie associée à l'événement a Onchange comme type d'évaluation, seules les modifications associées aux attributs figurant dans cette stratégie sont rejetées. L'événement proprement dit n'est pas rejeté et la stratégie suivante est évaluée.

Dans cet exemple, Stratégie 1, Stratégie 2 et Stratégie 3 ont toutes ALWAYS comme type d'évaluation de stratégie. La Stratégie 1 renvoie la valeur False, le processus de flux de travaux nommé Processus 1 n'est pas exécuté et aucune tâche n'est générée pour l'Utilisateur 1. Le contrôle d'événement est transmis immédiatement à la Stratégie 2. Les stratégies 2 et 3 renvoient toutes deux la valeur True. En raison de sa priorité plus élevée, le Processus 2 du flux de travaux est exécuté en premier et génère une tâche pour l'Utilisateur 2.

Si l'Utilisateur 2 approuve la tâche, le Processus 3 du flux de travaux est exécuté et génère une tâche pour l'Utilisateur 3, qui doit approuver la tâche pour l'événement à approuver. Ces actions sont présentées dans le tableau ci-dessous.

Priorité	Stratégie	Résultat	Flux de travaux	Approbateur	Action
1	Stratégie 1	False	Processus 1	Utilisateur 1	—
2	Stratégie 2	True	Processus 2	Utilisateur 2	Approuvé
3	Stratégie 3	True	Processus 3	Utilisateur 3	Approuvé

Toutefois, si l'Utilisateur 2 rejette la tâche, l'événement est rejeté et aucune tâche n'est générée pour l'Utilisateur 3, comme indiqué dans le tableau ci-dessous.

Priorité	Stratégie	Résultat	Flux de travaux	Approbateur	Action
1	Stratégie 1	False	Processus 1	Utilisateur 1	—
2	Stratégie 2	True	Processus 2	Utilisateur 2	Rejeté

Priorité	Stratégie	Résultat	Flux de travaux	Approbateur	Action
3	Stratégie 3	True	Processus 3	Utilisateur 3	—

Ensuite, Stratégie 1, Stratégie 2 et Stratégie 3 ont toutes ONCHANGE comme type d'évaluation de stratégie. Si l'Utilisateur 2 rejette la tâche, seules les modifications associées aux attributs figurant dans la Stratégie 2 sont rejetées. La Stratégie 3 est alors évaluée et le Processus de flux de travaux 3 est exécuté et génère une tâche pour l'Utilisateur 3. Si l'Utilisateur 3 rejette la tâche, l'événement est rejeté étant donné que toutes les modifications le concernant ont été rejetées. Si l'Utilisateur 3 approuve la tâche, l'événement est approuvé et les modifications d'attributs figurant dans la Stratégie 3 sont adoptées.

Priorité	Stratégie	Résultat	Flux de travaux	Approbateur	Action
1	Stratégie 1	False	Processus 1	Utilisateur 1	—
2	Stratégie 2	True	Processus 2	Utilisateur 2	Rejeté
3	Stratégie 3	True	Processus 3	Utilisateur 3	Approuvé

Description de la stratégie

Un attribut de description de chaîne facultatif ne pouvant pas faire l'objet d'une recherche a été ajouté à l'objet géré de la stratégie d'approbation et s'affiche dans les résultats de la tâche.

Nombre maximum de caractères pris en charge : 255 caractères

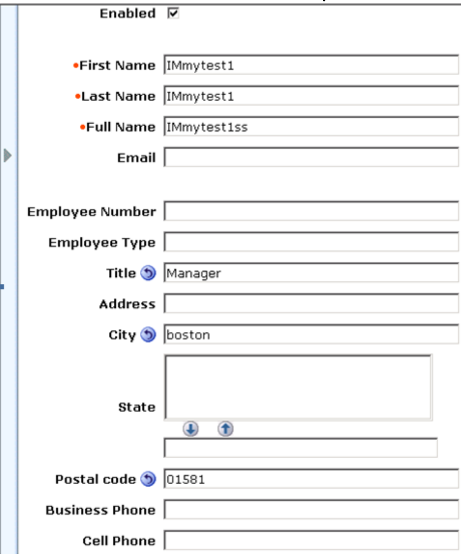
Vous pouvez entrer, pour la description, des informations de clé/de groupe au format suivant :

```
$ (bundle=<nom complet des groupes de ressources> : key=<clé>)
```

Mise en surbrillance des attributs modifiés dans les fenêtres d'approbation

Pour permettre à un approbateur de savoir quels attributs ont été modifiés ou d'annuler au besoin les changements apportés à ces attributs, une icône d'annulation a été ajoutée à la fenêtre du profil de l'approbateur pour indiquer à celui-ci que l'attribut en question a été changé.

L'approbateur peut consulter les valeurs initiales des attributs modifiables en cliquant sur le bouton d'annulation et peut en outre définir de nouvelles valeurs d'attribut.



Stratégies d'approbation et attributs à valeurs multiples

Précédemment, si vous aviez une règle configurée pour un attribut à valeurs multiples, il n'était pas possible de préciser que celle-ci ne devait s'exécuter que pour les valeurs récemment ajoutées ou supprimées. Ceci est désormais possible en regardant le type d'évaluation de stratégie pour un attribut à valeurs multiples. Si le type d'évaluation des règles est Onchange (Lors de la modification), cette règle peut uniquement être appliquée aux valeurs récemment ajoutées ou supprimées de l'attribut à valeurs multiples, et pas à toutes ses valeurs. Si la règle doit s'appuyer sur toutes les valeurs de l'attribut à valeurs multiples, qu'elles soient récemment ajoutées ou supprimées ou non, the type d'évaluation de la règle doit être Always (Toujours).

Les modifications apportées aux attributs à valeurs multiples apparaissent en surbrillance dans la fenêtre du profil, accompagnées d'une icône d'annulation. Si l'évaluation d'une règle renvoie la valeur true (vrai) parce qu'une valeur a été récemment ajoutée ou supprimée à un attribut à valeurs multiples, l'approbateur de ce changement voit TOUTES les valeurs contenues dans cet attribut. S'il clique sur l'icône d'annulation, il rétablit la valeur initiale de ce dernier. Si un approbateur souhaite voir les valeurs supprimées, il peut cliquer sur le bouton d'annulation pour afficher l'ensemble initial de valeurs. S'il clique sur l'icône de rétablissement de la modification, il affiche le nouvel ensemble de valeurs, ce qui lui permet de voir quelles sont les valeurs supprimées et celles ajoutées. S'il clique sur le bouton d'approbation, il accepte toutes les modifications apportées à cet attribut à valeurs multiples. S'il clique sur le bouton de rejet, il refuse toutes les modifications apportées à cet attribut à valeurs multiples. Aucune des règles suivantes liées à cet attribut ne sont évaluées, sauf en cas de nouveau changement de valeurs pour cet attribut.

Remarque : Concernant les règles basées sur des attributs à valeurs multiples, les valeurs contenues dans chaque attribut sont les valeurs réelles et non celles affichées. Par exemple, la valeur affichée pour l'état MA est Massachusetts. Lors de la création d'une stratégie d'approbation basée sur l'attribut d'état, la règle devrait avoir le format suivant : état=MA.

Prenons l'exemple des stratégies suivantes associées à l'événement ModifyUserEvent de la tâche d'administration Modifier un utilisateur.

Stratégie	Règle	Evaluation
Stratégie 1	Utilisateur où (état = MA)	OnChange
Stratégie 2	Utilisateur où (état = DC)	Always

La Stratégie 1 est évaluée chaque fois qu'un administrateur invoque la tâche ModifyUser pour changer l'attribut d'état et est évaluée comme vraie si la valeur MA est ajoutée ou supprimée de l'attribut d'état.

La stratégie 2 est évaluée chaque fois que l'administrateur invoque la tâche Modifier un utilisateur pour un utilisateur dont l'état contient la valeur DC.

Attributs marqués comme modifiés dans les fenêtres d'approbation du flux de travaux

Dans une fenêtre d'approbation, les attributs supplémentaires peuvent apparaître être marqués comme modifiés, même si l' administrateur ne les a pas modifiés dans la tâche d'origine. En effet, la fenêtre peut contenir des scripts qui peuvent changer les valeurs de divers attributs qu'elle contient lors de son initialisation ou de sa validation pour modifier un autre attribut.

Exemples de stratégies

Les cas d'utilisation métier suivants illustrent l'application de stratégies d'approbation de flux de travaux pour un événement.

Exemple 1 :

Cas d'utilisation : un administrateur modifie un compte de base de données relationnelle appartenant à un employé.

Tâche d'administration : ModifyMSSQLAccount

Evénement : ModifyMSSQLAccountEvent

Règle d'approbation : Utilisateur où (Titre = RDBAcctManager)

Processus de flux de travaux : ModAcctApproval (processus de flux de travaux personnalisé)

Objet : auteur de la tâche

Evaluation : toujours évaluer la règle

Exemple 2 :

Cas d'utilisation : un administrateur modifie le salaire d'un employé pour qu'il reflète une augmentation.

Tâche d'administration : Modifier un utilisateur

Evénement : ModifyUserEvent

Règle d'approbation : Utilisateur où (Salaire >= 100000)

Processus de flux de travaux : SalaryChangeApproval (processus de flux de travaux personnalisé)

Objet : objet principal de l'événement (utilisateur)

Evaluation : évaluer uniquement si l'attribut Salaire est modifié

Exemple 3 :

Cas d'utilisation : un administrateur ajoute un utilisateur au groupe Sous-traitants lorsque le titre de cet utilisateur devient Sous-traitant. Cet exemple peut être divisé en deux stratégies d'approbation.

Stratégie 1 :

Tâche d'administration : Modifier un utilisateur

Evénement : ModifyUserEvent

Règle d'approbation : Utilisateur où (Titre = Sous-traitant)

Processus de flux de travaux : SingleStepApproval (modèle de processus par défaut)

Objet : objet principal de l'événement (utilisateur)

Evaluation : évaluer uniquement si l'attribut Titre est modifié

Stratégie 2 :

Tâches d'administration : Modifier le groupe (ou Modifier l'appartenance au groupe)

Evénement : AddToGroup

Règle d'approbation : Groupe où (Nom du groupe = Sous-traitants)

Processus de flux de travaux : SingleStepApproval (modèle de processus par défaut)

Objet : objet secondaire de l'événement (groupe)

Evaluation : toujours évaluer la règle

Les cas d'utilisation métier suivants illustrent l'application des stratégies d'approbation de flux de travaux pour une tâche.

Exemple 1 :

Cas d'utilisation : un administrateur modifie un compte Active Directory appartenant à un employé.

Tâche d'administration : ModifyActiveDirectoryAccount

Objet : auteur de la tâche

Règle d'approbation : Utilisateur où (Titre = ActiveDirectoryManager)

Processus de flux de travaux : approbation en une seule étape

Evaluation : toujours évaluer la règle

Exemple 2 :

Cas d'utilisation : un administrateur modifie un utilisateur dont le code d'employé est HighSecurity.

Tâche d'administration : Modifier un utilisateur

Objet : objet principal de la tâche

Règle d'approbation : Utilisateur où (employeenumber = HighSecurity)

Processus de flux de travaux : approbation en une seule étape

Evaluation : toujours évaluer la règle

Exemple 3 :

Cas d'utilisation : un administrateur modifie un utilisateur pour affecter les rôles d'administration CheckApprover et CheckSigner.

Tâche d'administration : Modifier un utilisateur

Objet : violation d'une stratégie d'identité

Règle d'approbation : IdentityPolicy où (Nom = CheckRoles)

Processus de flux de travaux : approbation en une seule étape

Evaluation : toujours évaluer la règle

Configuration du flux de travaux utilisant des stratégies pour les événements

La procédure de configuration du flux de travaux utilisant des stratégies est similaire à la procédure de configuration du flux de travaux de niveau événement et comprend en outre une étape de définition des stratégies d'approbation qui déterminent si le flux de travaux est exécuté.

Pour configurer un flux de travaux utilisant les stratégies

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration (ou Créer une tâche d'administration).

   Une fenêtre Sélectionner une tâche d'administration apparaît.

2. Recherchez la tâche que vous souhaitez placer sous contrôle du flux de travaux et cliquez sur Sélectionner.

   Une fenêtre Modifier la tâche d'administration (ou Créer une tâche d'administration) apparaît.

3. Dans l'onglet Profil, vérifiez que l'option Activer le flux de travaux est activée.

4. Dans l'onglet Evénements, sélectionnez un événement à mapper vers un modèle de processus.

   La fenêtre de mappage du flux de travaux apparaît.

5. Activez la case d'option Utilisant des stratégies, puis cliquez sur Ajouter.

   La fenêtre Stratégie d'approbation s'ouvre.

6. Configurez une stratégie d'approbation (page 487).

7. Configurez les outils de résolution de participants en fonction du processus de flux de travaux sélectionné.

   Les requêtes de participants sont ajoutées au processus.

8. Cliquez sur OK.

   CA IdentityMinder enregistre votre configuration de flux de travaux de niveau événement.

9. Cliquez sur Soumettre.

   CA IdentityMinder traite la modification de tâche.

Remarque : La liste de processus de flux de travaux comprend des processus à utiliser selon la méthode des modèles et la méthode WorkPoint :

- quand un processus de méthode de modèles est sélectionné (SingleStepApproval ou TwoStageApprovalProcess), la page se développe pour permettre la configuration de l'outil de résolution de participants ;
- quand un processus de méthode WorkPoint est sélectionné, la page ne se développe pas. Les outils de résolution de participants se configurent dans WorkPoint Designer.

Informations complémentaires :

Configuration d'une stratégie d'approbation (page 487)
Outils de résolution de participants : méthode des modèles (page 432)
Outils de résolution de participants : méthode Workpoint (page 452)

Configuration du flux de travaux utilisant des stratégies pour les tâches

La procédure de configuration du flux de travaux utilisant des stratégies pour les tâches est similaire à la procédure de configuration du flux de travaux de niveau tâche, excepté qu'elle comprend en outre des étapes de définition des stratégies d'approbation qui déterminent si le flux de travaux est exécuté.

Pour configurer un flux de travaux utilisant des stratégies

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration (ou Créer une tâche d'administration).

   Une fenêtre Sélectionner une tâche d'administration apparaît.

2. Recherchez la tâche que vous souhaitez placer sous contrôle du flux de travaux et cliquez sur Sélectionner.

   Une fenêtre Modifier la tâche d'administration (ou Créer une tâche d'administration) apparaît.

3. Dans l'onglet Profil, vérifiez que l'option Activer le flux de travaux est activée

4. Sous l'onglet Profil, cliquez sur l'icône crayon en regard du champ Processus de flux de travaux

   La fenêtre de mappage du flux de travaux apparaît.

5. Activez la case d'option Utilisant des stratégies, puis cliquez sur Ajouter.

   La fenêtre Stratégie d'approbation s'ouvre.

6. Configurez une stratégie d'approbation (page 487).

7. Configurez les outils de résolution de participants en fonction du processus de flux de travaux sélectionné.

   Les requêtes de participants sont ajoutées au processus.

8. Cliquez sur OK.

   CA Identity Manager enregistre votre configuration de flux de travaux de niveau tâche.

9. Cliquez sur Soumettre.

   CA Identity Manager traite la modification de tâche.

Remarque: La liste des processus de flux de travaux inclut des processus à utiliser avec la méthode des modèles pour le flux de travaux utilisant des stratégies de niveau tâche.

- Quand un processus de méthode des modèles est sélectionné (SingleStepApproval ou TwoStageApprovalProcess), la page se développe pour permettre la configuration de l'outil de résolution de participants.

Informations complémentaires

Configuration d'une stratégie d'approbation (page 487)

Configuration d'une stratégie d'approbation

La configuration d'une stratégie d'approbation pour un événement ou une tâche implique la procédure suivante.

1. Sélectionnez un objet à tester.
2. Définissez une règle d'approbation pour l'objet.
3. Pour les objets principaux, indiquez s'il s'agit d'une évaluation conditionnelle.
4. Entrez l'ordre de l'évaluation des stratégies.
5. Configurez un processus de flux de travaux à exécuter si la règle est vérifiée.

Pour configurer une stratégie d'approbation

1. Dans la fenêtre Stratégie d'approbation, sélectionnez un objet pour la règle à tester dans la liste déroulante.

   La fenêtre se modifie selon votre sélection.
2. Dans la liste déroulante située à côté du nom de l'objet, sélectionnez un modèle d'expression de condition.

   La fenêtre se modifie selon votre sélection.
3. Créez et modifiez votre expression de condition.
4. Activez la case d'option Evaluation des règles pour indiquer si la règle doit toujours être évaluée ou si elle doit l'être uniquement lorsqu'un attribut de la condition d'approbation est modifié.
5. Entrez une valeur entière positive pour spécifier l'ordre de l'évaluation des stratégies (lorsque l'événement est associé à plusieurs stratégies).
6. Sélectionnez et configurez le processus de flux de travaux qui est exécuté si la règle est évaluée comme vraie.
7. Cliquez sur OK afin d'enregistrer la stratégie d'approbation.

Informations complémentaires :

Configuration du flux de travaux utilisant des stratégies pour les événements (page 484)
Configuration du flux de travaux utilisant des stratégies pour les tâches (page 486)
Configuration d'un flux de travaux au niveau événement (page 431)

Etat du flux de travaux utilisant des stratégies

L'administrateur CA IdentityMinder peut afficher l'état des tâches contenant des stratégies d'approbation de flux de travaux à l'aide des outils système standard suivants.

- Onglet Afficher les tâches soumises
- Onglet Historique de l'utilisateur
- Rapports et journaux

Les informations sur les tâches soumises et l'historique des tâches sont les suivantes.

- Informations sur les tâches et les événements
- Informations sur les flux de travaux et les règles d'approbation
- Résultats de l'évaluation des règles d'approbation

Pour obtenir une description de l'historique des tâches soumises, consultez la documentation de l'onglet Système.

Informations complémentaires :

Statut des tâches dans CA IdentityMinder (page 598)
Description de l'état d'événement (page 605)

Mappage de flux de travaux utilisant une stratégie globale de niveau événement

Un événement peut être mappé vers un processus de flux de travaux à partir de la console de gestion ou être associé à des stratégies d'approbation de flux de travaux utilisant une stratégie dans une tâche spécifique. La nouvelle tâche Configurer le flux de travaux utilisant des stratégies globales pour les événements permet aux administrateurs de définir un mappage de flux de travaux utilisant une stratégie pour les événements au niveau de l'environnement. Contrairement aux flux de travaux utilisant une stratégie qui sont définis pour un événement dans une tâche d'administration, les mappages de flux de travaux utilisant une stratégie sont appliqués à toutes les tâches qui génèrent l'événement concerné.

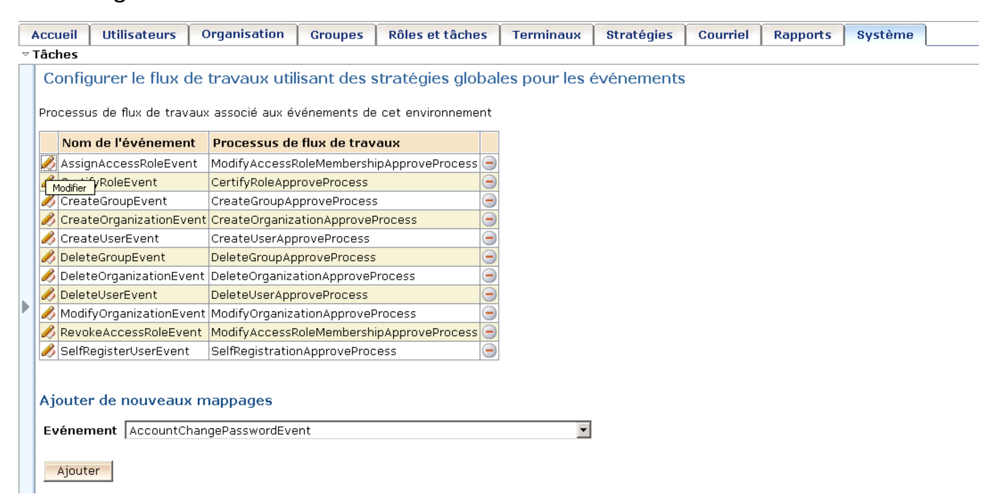
Remarque : La tâche Configurer le flux de travaux utilisant des stratégies globales pour les événements fonctionne uniquement lorsque le flux de travaux est activé. L'exécution de cette tâche lorsque le flux de travaux est désactivé génère une erreur.

Cette tâche a été ajoutée à l'onglet Système. En cas de soumission d'une tâche, le processus de flux de travaux de chaque événement qu'elle contient est récupéré de la manière suivante.

Tout flux de travaux configuré pour l'événement de cette tâche d'administration est prioritaire. Un événement peut être configuré pour un flux de travaux qui utilise une stratégie ou pour un qui n'en utilise pas. Si c'est un flux de travaux utilisant une stratégie qui est configuré pour l'événement de cette tâche d'administration, le processus de flux de travaux associé à la stratégie est appelé. Si aucune règle n'est respectée, aucun flux de travaux n'est sollicité pour l'événement. De la même manière, s'il le flux de travaux configuré pour l'événement de cette tâche d'administration n'utilise pas de stratégie, le processus de flux de travaux associé à la stratégie est appelé. Si aucun flux de travaux n'est configuré pour l'événement de cette tâche d'administration, la configuration de flux de travaux globale pour cet événement est prioritaire.

Fenêtre de tâche Configurer le flux de travaux utilisant des stratégies globales pour les événements

La tâche Configurer le flux de travaux utilisant des stratégies globales pour les événements permet à un administrateur de configurer un flux de travaux utilisant ou non des stratégies pour tous les événements de l'environnement actuel. Si vous cliquez sur la tâche, vous voyez le mappage des événements par défaut vers les définitions de processus de flux de travaux. Chaque mappage d'événement peut être modifié ou supprimé et il est possible d'en ajouter de nouveaux pour les événements qui n'ont pas été configurés.



Les champs de cette fenêtre sont répertoriés ci-dessous.

Processus de flux de travaux associé aux événements de cet environnement

Spécifie les processus de flux de travaux associés aux stratégies d'approbation.

Ajouter de nouveaux mappages

Spécifie une stratégie d'approbation à mapper vers un processus de flux de travaux.

Bouton Ajouter

Ajoute le nouveau mappage.

L'ajout ou la modification d'un mappage ouvre la fenêtre Mappage du flux de travaux qui permet de sélectionner les mappages de processus et les stratégies d'approbation. Le comportement est identique à la configuration de flux de travaux de niveau événement. Si vous cliquez sur le bouton Ajouter de la page Mappage du flux de travaux, une autre page s'affiche et vous permet de configurer une stratégie d'approbation.

Informations complémentaires

Configuration du flux de travaux utilisant des stratégies pour les événements (page 484)
Configuration d'une stratégie d'approbation (page 487)

Configurer le flux de travaux utilisant des stratégies globales pour les événements

Configurez cet onglet pour le flux de travaux utilisant des stratégies globales pour les événements.

Nom

Nom que vous affectez à l'onglet.

Balise

Identifiant unique pour l'onglet au sein de la tâche. La balise doit commencer par une lettre ou un caractère de soulignement et contenir uniquement des lettres, des chiffres et des caractères de soulignement. La balise est principalement utilisée pour la définition de valeurs de données via des documents XML ou des paramètres HTTP.

Masquer l'onglet

Empêche que l'onglet soit visible dans la tâche. Cette option est utile pour les applications qui doivent masquer l'onglet, mais qui ont toujours accès aux attributs de cet onglet.

Fenêtre de recherche d'utilisateurs

Définit la fenêtre de recherche à utiliser pour afficher des utilisateurs.

Fenêtre de liste d'utilisateurs

Définit la fenêtre qui détermine les colonnes et le tri sous cet onglet.

Fenêtre de recherche de groupes

Définit la fenêtre de recherche à utiliser pour afficher les groupes.

Fenêtre de liste de groupes

Définit la fenêtre qui détermine les colonnes et le tri sous cet onglet.

Fenêtre de recherche de rôles d'administration

Définit la fenêtre de recherche à utiliser pour afficher les rôles d'administration.

Fenêtre de liste de rôles d'administration

Définit la fenêtre qui détermine les colonnes et le tri sous cet onglet.

Fenêtre de recherche de tâches d'administration

Définit la fenêtre de recherche à utiliser pour afficher les tâches d'administration.

Fenêtre de liste de tâches d'administration

Définit la fenêtre qui détermine les colonnes et le tri sous cet onglet.

Requêtes en ligne

Identity Manager vous permet de créer des tâches de requêtes générales en ligne. L'implémentation par défaut de la requête en ligne se compose d'un ensemble de tâches associées pour les requêtes d'automodification et les requêtes de modification administrative d'utilisateur. Cependant, la fonctionnalité de requête en ligne pourrait facilement être implémentée pour d'autres tâches de requêtes d'Identity Manager.

Une requête de modification d'utilisateur déclenche un processus de flux de travaux qui génère une tâche. Les participants au flux de travaux peuvent approuver et implémenter la tâche ou bien la rejeter. L'utilisateur commençant la tâche saisit une description de la requête dans l'éditeur d'historique, une zone de texte qu'Identity Manager utilise pour conserver un historique de la requête. Cet éditeur d'historique peut être configuré pour permettre aux participants de laisser des commentaires concernant l'action qu'ils réalisent sur la tâche. Ces commentaires sont intégrés dans l'historique cumulé de la tâche.

De nouvelles actions outre les actions standard d'approbation ou de rejet (ou à leur place) sont également possibles. Par exemple, un participant commercial peut clarifier ou commenter la requête et un participant technique peut implémenter la requête. Ces nouvelles activités peuvent être représentées par de nouveaux boutons d'actions de flux de travaux comme Commenter et Implémenter, que vous pouvez ajouter aux boutons standard Approuver et Rejeter dans la tâche d'approbation.

Tâches de requêtes en ligne

Il y a cinq tâches qui fonctionnent conjointement pour constituer l'implémentation de la requête par défaut en ligne. Ces tâches montrent le fonctionnement des requêtes personnalisées, de l'historique et des boutons d'action du flux de travaux.

Remarque : Les tâches administratives (Modifier mon compte et Créer une requête en ligne) sont configurées par défaut pour des flux de travaux au niveau événement utilisant le modèle de processus de consultation..

Modifier mon compte

Il s'agit d'une tâche administrative d'automodification qui crée une requête de modification d'un compte d'utilisateur. Elle inclut un onglet Requête, avec un éditeur d'historique pour décrire la requête, et un onglet Profil pour des informations utilisateur en lecture seule.

Créer une requête en ligne

Il s'agit d'une tâche administrative de modification d'utilisateur qui crée une requête de modification de compte pour un utilisateur particulier. Elle inclut un onglet Requête, avec un éditeur d'historique pour décrire la requête, et un onglet Profil sujet pour des informations utilisateur en lecture seule.

Approuver une requête en ligne

Il s'agit d'une tâche d'approbation qui permet au participant commercial d'approuver ou de rejeter la tâche ou bien de demander d'autres renseignements sur la tâche. Cette tâche inclut un onglet Requête, avec un affichage de l'historique et un éditeur d'historique pour des demandes ou commentaires, un onglet Profil sujet en lecture seule et un onglet Destinataires.

Commenter une requête en ligne

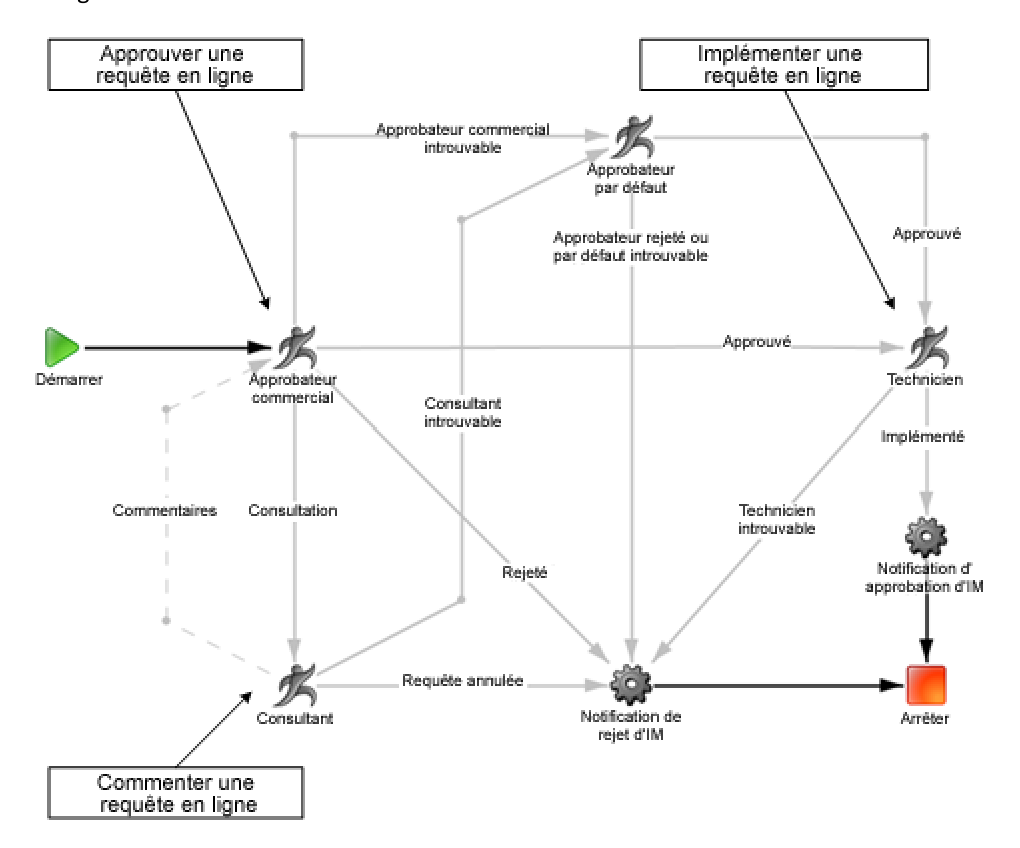
Il s'agit d'une tâche d'approbation qui permet au participant en charge de répondre à une requête de renseignements et de retourner la tâche au participant commercial pour approbation. Elle inclut un onglet Requête, avec un affichage de l'historique et un éditeur d'historique pour des commentaires et un onglet Profil sujet en lecture seule.

Implémenter une requête en ligne

Il s'agit d'une tâche d'approbation qui permet au participant technique d'implémenter la tâche et d'ajouter un commentaire dans l'historique de la tâche. Elle inclut un onglet Implémenter une requête, avec un affichage de l'historique et un éditeur d'historique pour des commentaires, un onglet Profil sujet en lecture seule et un onglet Destinataires.

Processus de requêtes en ligne

Les tâches de requêtes en ligne sont contrôlées par un modèle de processus de flux de travaux appelé Processus de consultation, présenté tel qu'il apparaît dans WorkPoint Designer :



Le processus de consultation inclut quatre activités manuelles correspondant aux tâches d'approbation dans l'implémentation de la requête en ligne :

- une activité pour l'approbateur commercial, qui rejette la tâche, approuve la tâche et la transmet au technicien ou demande d'autres renseignements au consultant ;
- une activité pour le consultant, qui répond aux questions sur la tâche et la renvoie à l'approbateur technique ;
- une activité pour l'approbateur par défaut, qui prend la tâche en charge si ni l'approbateur technique, ni le consultant ne sont joignables ;
- une activité pour le technicien, qui implémente la requête et termine la tâche.

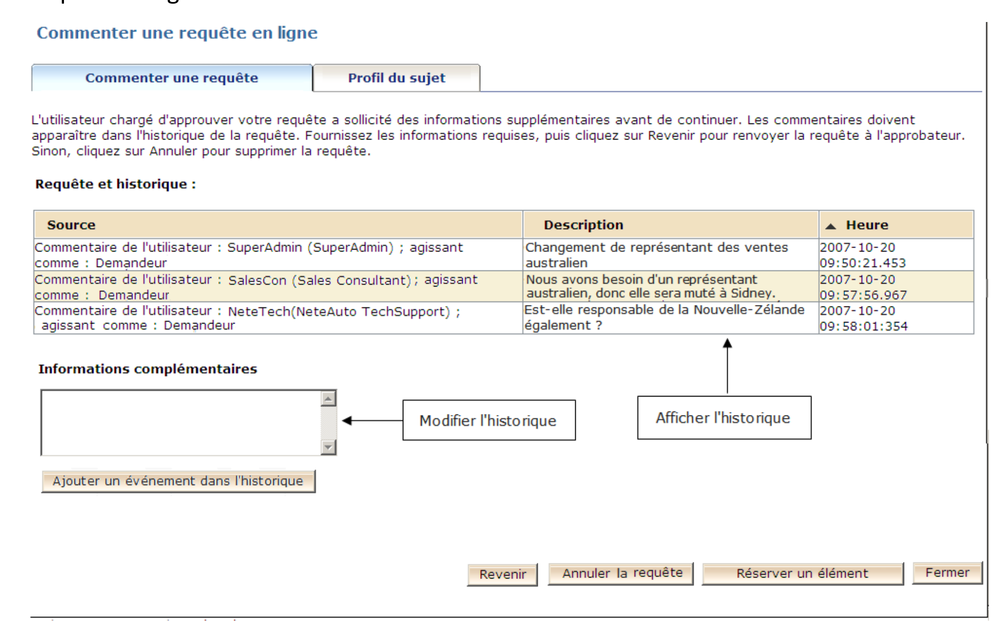
Historique de requête en ligne

La fonction historique de la requête en ligne permet aux participants de créer un enregistrement des actions de la tâche. La responsabilité de la tâche passant d'un participant à un autre, le nouveau participant est capable de vérifier l'historique de la tâche avant d'entreprendre une action.

Deux contrôles sont utilisés pour implémenter l'historique de la requête en ligne :

- L'affichage de l'historique est un tableau en lecture seule, qui contient des détails des entrées précédentes par ordre chronologique ;
- L'éditeur d'historique est une zone de texte pour créer de nouvelles entrées d'historique. Il est aussi doté d'un bouton facultatif pour ajouter plusieurs entrées sans soumettre la tâche.

Par défaut, l'éditeur d'historique et l'affichage d'historique apparaissent dans l'onglet Requête pour toutes les tâches associées à l'implémentation de la requête en ligne. La fenêtre suivante illustre les contrôles de l'historique dans la tâche Commenter la requête en ligne :



Utilisation des requêtes en ligne

Les étapes suivantes décrivent le processus de flux de travaux des requêtes en ligne. Pour chaque étape, la tâche générée dans IM figure entre parenthèses. A chaque étape du processus, le participant peut ajouter un commentaire dans l'éditeur d'historique. Ce commentaire apparaît dans l'affichage de l'historique pour le nouveau participant dans le processus de flux de travaux.

1. L'initiateur de la tâche demande une modification à un utilisateur d'IM (Créer une requête en ligne).
2. L'approbateur commercial reçoit une tâche et effectue l'une des missions suivantes :
   - Approuve la tâche (Approuver la requête en ligne).
   - Rejette la tâche et termine le processus de flux de travaux. Aucune nouvelle tâche n'est générée.
   - Demande des renseignements au consultant (Commenter une requête en ligne).
3. Le consultant reçoit une tâche et effectue l'une des missions suivantes :
   - Ajoute un commentaire et retourne la tâche à l'approbateur commercial. Aucune nouvelle tâche n'est générée.
   - Annule la tâche et termine le processus de flux de travaux. Aucune nouvelle tâche n'est générée.
4. Le technicien reçoit une tâche et implémente la requête (Implémenter la requête en ligne).

Boutons d'action du flux de travaux

Les tâches d'approbation dans Identity Manager ont historiquement leurs boutons d'action Approuver et Rejeter qui apparaissent dans les fenêtres correspondantes des tâches. Les boutons d'action du flux de travaux permettent aux administrateurs de développer la fonctionnalité des tâches et flux de travaux d'Identity Manager en ajoutant des boutons aux tâches d'approbation et en supprimant ou modifiant des boutons existants. Les boutons standard Approuver et Rejeter sont implémentés de la même manière que les boutons d'action personnalisés des flux de travaux.

Par exemple, un processus de flux de travaux peut nécessiter une action permettant à des participants de niveau moyen de transmettre certains cas à un participant de la direction pour une approbation ou un rejet final. Ces participants de niveau moyen pourraient ajouter un commentaire ou des recommandations au moyen de l'éditeur d'historique et envoyer ensuite la tâche au participant de la direction pour qu'il analyse la tâche et l' approuve ou la rejette.

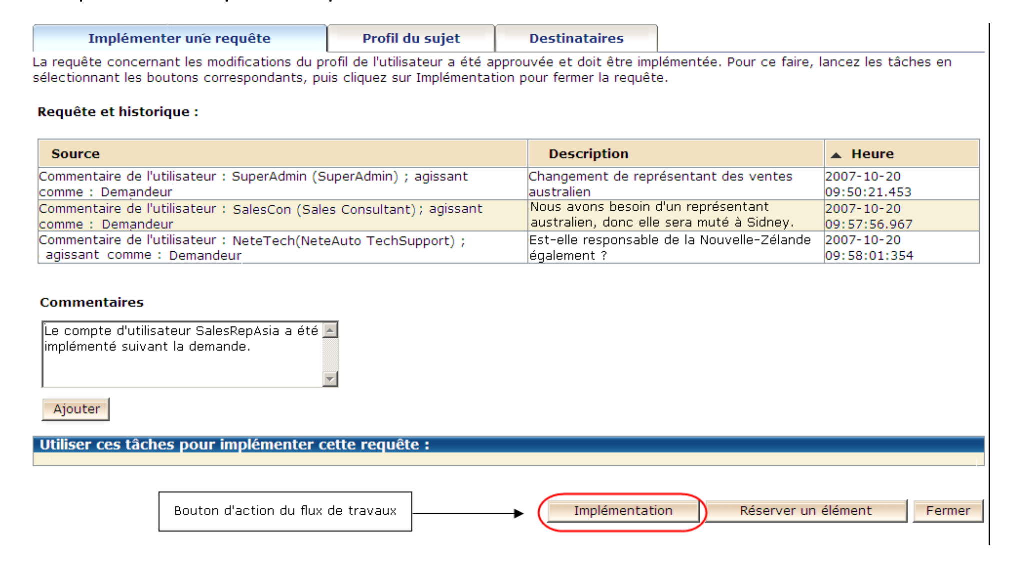
L'ajout ou la suppression de boutons d'action du flux de travaux requiert des changements appropriés dans le processus de flux de travaux de WorkPoint qui fournissent les tâches métier pour le traitement de ces actions.

Informations complémentaires :

Boutons de flux de travaux dans les tâches d'approbation (page 497)
Configuration des boutons dans CA IdentityMinder (page 497)
Configuration des boutons dans WorkPoint Designer (page 500)

Boutons de flux de travaux dans les tâches d'approbation

Les boutons d'action du flux de travaux correspondent à des noeuds de transition s'éloignant des noeuds d'activité manuelle dans un diagramme de processus de WorkPoint. Par exemple, dans le processus de consultation, le noeud d'activité du technicien a une seule transition appelée Implémentée. Elle correspond au bouton Implémentation dans la tâche d'approbation Implémenter une requête en ligne, qui est indiqué dans la capture ci-après :



Remarque : Les boutons Réserver un élément et Fermer sont régis par la logique de programmation CA IdentityMinder et non par le contrôle du flux de travaux.

Informations complémentaires :

Boutons d'action du flux de travaux (page 496)
Configuration des boutons dans CA IdentityMinder (page 497)

Configuration des boutons dans CA IdentityMinder

Pour configurer un bouton d'action du flux de travaux, cliquez sur le bouton nommé Boutons d'action du flux de travaux dans l'onglet Profil d'une tâche d'approbation.

Le bouton de l'onglet Profil a un tableau avec une ligne pour chaque bouton d'action du flux de travaux. Chaque ligne de bouton a les quatre propriétés suivantes, qui correspondent aux colonnes dans le tableau :

Nom d'affichage

Le nom qui apparaît sur le bouton dans l'écran d'approbation. Il s'agit d'une valeur localisée sous certaines conditions, qui peut être une chaîne ou une clé pour une chaîne localisée dans un fichier de ressources.

Action

Valeur renvoyée dans le processus de flux de travaux lorsque l'option est sélectionnée. Cette valeur est un attribut du noeud de transition correspondant dans le diagramme de processus de WorkPoint. La valeur est une chaîne non localisée. Les paramètres par défaut sont approuvés et rejetés.

Infobulle

Brève description de l'action du bouton, qui apparaît quand un utilisateur place le curseur de la souris sur le bouton. Il s'agit d'une valeur localisée sous certaines conditions, qui peut être une chaîne ou une clé pour une chaîne localisée dans un fichier de ressources.

Description longue

Une description plus longue de l'action du bouton qui ajoute un message décrivant l'action dans l'écran Afficher la tâche soumise. Si la description est vide, le message affiché dans la fenêtre Afficher les tâches soumises correspond au nom du bouton. Il s'agit d'une valeur localisée sous certaines conditions, qui peut être une chaîne ou une clé pour une chaîne localisée dans un fichier de ressources.

Informations complémentaires :

Configuration des boutons dans WorkPoint Designer (page 500)

Ajout de boutons du flux de travaux

Pour ajouter un nouveau bouton à un processus de flux de travaux existant, suivez les étapes détaillées suivantes :

1. Ajoutez le bouton de flux de travaux dans Identity Manager.

   Vous trouverez des instructions dans la rubrique Ajouter un bouton d'action du flux de travaux (page 499).

2. Le cas échéant, ajoutez des clés de localisation.

   Vous trouverez des instructions dans le *manuel de configuration*.

3. Ajoutez tous les nouveaux noeuds requis dans WorkPoint Designer.

   Vous trouverez des instructions dans l'aide en ligne de WorkPoint Designer.

4. Définissez un script dans un noeud de transition de WorkPoint Designer.

   Vous trouverez des instructions dans la rubrique Configuration des boutons dans WorkPoint Designer (page 500).

Informations complémentaires :

Ajouter un bouton d'action du flux de travaux. (page 499)
Configuration des boutons dans WorkPoint Designer (page 500)

Ajouter un bouton d'action du flux de travaux.

Vous pouvez ajouter des boutons d'action du flux de travaux aux tâches d'approbation dans CA IdentityMinder.

Pour ajouter un bouton d'action du flux de travaux à une tâche administrative.

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.

   La fenêtre Sélectionner une tâche d'administration apparaît.

2. Rechercher la tâche d'approbation et cliquez sur Sélectionner.

   La fenêtre Sélectionner une tâche d'administration apparaît.

3. Dans l'onglet Profil, cliquez sur le bouton nommé Boutons d'action du flux de travaux.

   Le bouton d'action du processus de l'onglet Profil apparaît.

4. Cliquez sur Ajouter un bouton pour ajouter un nouveau bouton à la tâche d'approbation.

5. Saisissez les informations de propriétés du bouton.

6. Cliquez sur OK.

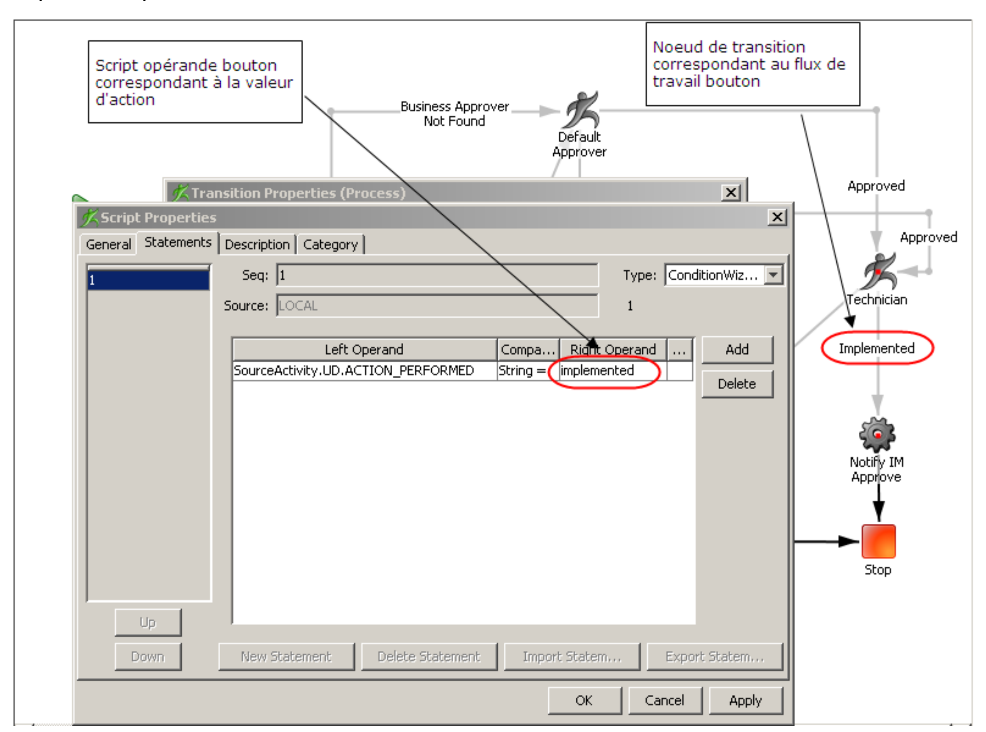
   CA IdentityMinder enregistre les informations du nouveau bouton.

7. Cliquez sur Soumettre.

   CA IdentityMinder traite la modification de tâche.

Configuration des boutons dans WorkPoint Designer

Dans WorkPoint Designer, les boutons d'action du flux de travaux sont configurés au moyen des propriétés des scripts des noeuds de transition, comme indiqué dans la capture ci-après.



Par défaut, les boutons d'action du flux de travaux utilisent les propriétés de script suivantes pour effectuer une comparaison de chaînes :

- Opérande gauche : ACTION_PEFORMED, qui est définie dans les propriétés des Données de l'utilisateur du noeud d'activité précédent.
- Opérande droite : valeur Action de ce bouton, qui est définie dans le bouton de l'onglet Profil de la console d'utilisateur.

Remarque : Reportez-vous à l'aide en ligne de WorkPoint Designer pour des informations sur les scripts et propriétés de noeuds d'activité et de transition.

Informations complémentaires :

Configuration des boutons dans CA IdentityMinder (page 497)

Listes de travail et tâches

Une *liste de travail* est une liste de tâches (d'approbation ou autres) qui apparaît dans la console d'utilisateur du participant autorisé à approuver les tâches. Les tâches correspondent à des activités manuelles au cours d'un processus de flux de travaux. Elles sont représentées sous forme de lignes dans la liste de travail.

Des tâches peuvent être ajoutées à une liste de travail comme suit.

- Un outil de résolution de participants détermine la liste des approbateurs.
- Un autre utilisateur envoie des tâches déléguées.
- La tâche est réaffectée à un autre utilisateur.

Des tâches peuvent être supprimées d'une liste de travail comme suit.

- La tâche est terminée (approuvée ou rejetée).
- La tâche est réaffectée à un autre utilisateur.
- La tâche est réservée. Elle est alors supprimée de la liste de travail de tous les autres participants.

Remarque : Lorsque vous acceptez ou rejetez une tâche, la modification n'est pas instantanée. Par exemple, si vous rejetez une tâche, elle apparaît toujours dans votre liste de travail jusqu'à ce que le processus de flux de travaux enregistre l'information et amène le processus au prochain noeud.

Les onglets d'information qui apparaissent pour une tâche varient selon que cette dernière a été générée par un flux de travaux sous contrôle au niveau tâche ou au niveau événement.

- **Profil** : fournit des informations de profil sur l'objet affecté par l'événement (niveau événement uniquement).
- **Détails de la tâche** : fournit des informations détaillées pour tous les événements de la tâche (niveau tâche uniquement).
- **Approbateurs** : liste tous les approbateurs et délégateurs individuels pour la tâche ou l'événement (niveau tâche ou événement).

Affichage d'une liste de travail

Votre liste de travail apparaît automatiquement lorsque vous vous connectez à la console d'utilisateur si vous avez été affecté en tant que participant à des tâches d'approbation commencées par d'autres utilisateurs.

Pour afficher manuellement votre liste de travail

1. Dans la console d'utilisateur, sélectionnez Accueil, Afficher ma liste de travail.

   Votre liste de travail apparaît.

2. Cliquez sur le nom d'une tâche pour l'afficher.

   La tâche sélectionnée apparaît.

Les administrateurs peuvent gérer les tâches des utilisateurs pour lesquels ils sont habilités.

Remarque : La gestion des tâches d'un utilisateur permet aux administrateurs de réserver une tâche. Le fait d'afficher la liste de travail d'un utilisateur n'autorise d'aucune manière à modifier les tâches.

Pour afficher la liste de travail d'un autre utilisateur

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, Gérer les tâches, Afficher la liste de travail de l'utilisateur.

   Une fenêtre de sélection des utilisateurs apparaît.

2. Cherchez l'utilisateur dont vous souhaitez voir la liste de travail et cliquez sur Sélectionner.

   La liste de travail de l'utilisateur s'affiche à l'écran.

Pour gérer les tâches d'un autre utilisateur

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, Gérer les tâches, Gérer les tâches de l'utilisateur.

   Une fenêtre de sélection des utilisateurs apparaît.

2. Cherchez l'utilisateur dont vous souhaitez gérer les tâches et cliquez sur Sélectionner.

   La liste de travail de l'utilisateur s'affiche à l'écran.

3. Cliquez sur le nom d'une tâche pour l'afficher.

   La tâche sélectionnée apparaît.

Réservation des tâches

Vous pouvez réserver une tâche pour la "consulter" et la supprimer de la liste de travail des autres participants. Le fait de réserver une tâche conserve la tâche pour l'utilisateur qui effectue la réservation.

Si l'utilisateur qui a réservé la tâche la libère, elle redevient disponible sur la liste de travail des autres participants. Si l'utilisateur qui a réservé la tâche l'approuve ou la rejette, elle est terminée et n'est plus disponible pour les autres participants.

Informations complémentaires :

Délégation et tâches réservées (page 503)
Réaffectation et tâches réservées (page 503)

Réaffectation et tâches réservées

Si un utilisateur a réservé une tâche et qu'elle est réaffectée, il conserve cette tâche. Cependant si l'utilisateur la libère ensuite, il ne peut plus y accéder après.

Un administrateur peut réaffecter, réserver ou libérer la tâche d'un autre utilisateur mais il ne peut pas approuver ou rejeter la tâche d'un autre utilisateur. Seul le participant à qui la tâche a été affectée a cette faculté.

Informations complémentaires :

Réaffectation de tâches (page 510)

Délégation et tâches réservées

Tant que la délégation est active, le délégué ou le délégateur peut réserver une tâche. Une tâche réservée par un utilisateur ne peut pas apparaître sur la liste de travail d'un autre utilisateur.

Par exemple, si un délégué a une tâche réservée alors que la délégation a été supprimée, il conserve la tâche réservée. Cependant si le délégué la libère ensuite, il ne peut plus y accéder après.

Si un utilisateur qui est un délégué est supprimé alors qu'il a une tâche réservée, il conserve encore la tâche. Si le délégué approuve ensuite la tâche, l'audit ne peut plus déterminer qui l'a déléguée.

Si un délégué a une tâche réservée alors que la délégation a été supprimée, il conserve l'accès jusqu'à ce que la tâche soit terminée ou libérée.

Informations complémentaires :

Réservation des tâches (page 503)
Délégation de tâches (page 504)

Réserver ou libérer une tâche

Vous réservez une tâche pour la "consulter" et la supprimer de la liste de travail des autres participants.

Vous libérez une tâche réservée pour la rendre disponible sur la liste de travail des autres participants.

Remarque : La seule façon de libérer une tâche réservée est de la libérer de manière explicite.

Pour réserver ou libérer une tâche

1. Dans la console d'utilisateur, sélectionnez Accueil, Afficher ma liste de travail.

   Votre liste de travail apparaît.

2. Sélectionnez la tâche que vous souhaitez réserver ou libérer.

   La fenêtre développé de la tâche apparaît.

3. Cliquez sur Réserver un élément ou Libérer un élément.

   CA IdentityMinder confirme votre action.

Délégation de tâches

La *délégation* de tâches permet à un utilisateur (le délégateur) d'indiquer qu'un autre utilisateur (le délégué) est autorisé à approuver des tâches dans la liste de travail du délégateur. Un délégateur peut affecter des tâches à un autre utilisateur pendant des périodes où il est absent. Les délégateurs conservent l'accès total à leurs tâches pendant la période de délégation.

Les tâches déléguées ne sont absolument pas modifiées. La connexion indique si une tâche a été déléguée.

La délégation fonctionne en permettant au délégué "d'usurper" l'identité du délégateur et d'afficher les éléments sur la liste de travail du délégateur. Lors de l'affichage d'une liste de travail, les délégués voient leurs propres tâches, ainsi que celles du délégateur.

La délégation n'est pas transitive. Un délégué peut uniquement voir les tâches que le délégateur lui a affectées directement. Par exemple, si l'utilisateur A délègue des tâches à l'utilisateur B et que cet utilisateur B délègue des tâches à l'utilisateur C, ce dernier peut uniquement voir les tâches appartenant à l'utilisateur B mais pas les tâches qui ont pu être déléguées à l'utilisateur B par l'utilisateur A.

Informations complémentaires :

Délégation et tâches réservées (page 503)

Attribut réservé de la délégation

La délégation utilise l'attribut réservé suivant :

%DELEGATORS%

Cet attribut réservé enregistre les noms des utilisateurs qui sont délégués des utilisateurs avec l'attribut, ainsi que l'heure de création de la délégation.

Activation de la délégation

Vous devez disposer de la délégation d'approbation de flux de travaux activée avant de pouvoir utiliser une tâche déléguée par un autre utilisateur. Par défaut, la délégation est désactivée.

Pour activer la délégation d'approbation de flux de travaux

1. Pour ouvrir la console de gestion, saisissez l'URL suivante dans un navigateur.

   `http://hostname/iam/immanage`

   hostname

   Définit le nom de domaine complet du serveur sur lequel CA IdentityMinder est installé. Par exemple, monserveur.masociété.com:port.

2. Cliquez sur Environnements, puis sélectionnez le nom de l'environnement CA IdentityMinder approprié.

3. Cliquez sur Paramètres avancés puis sur Délégation de l'approbation de flux de travaux.

4. Activez la case à cocher Activé, puis cliquez sur Enregistrer.

Informations complémentaires :

Réalisation d'une délégation personnelle (page 506)
Délégation à un autre utilisateur (page 509)

Réalisation d'une délégation personnelle

Vous pouvez déléguer des tâches à un autre utilisateur pendant des périodes où vous êtes absent. Les délégateurs conservent toujours l'accès total à leurs tâches pendant la période de délégation.

Pour déléguer personnellement des tâches

1. Dans la console d'utilisateur, sélectionnez Accueil, Gestionnaire d'absence du bureau.

   La fenêtre du Gestionnaire d'absence du bureau apparaît.

2. Cliquez sur Ajouter un utilisateur.

   Une fenêtre de sélection des utilisateurs apparaît.

3. Cherchez et sélectionnez un ou plusieurs utilisateurs comme délégués.

   Les utilisateurs sont ajoutés à la liste de délégués.

4. Cliquez sur Soumettre.

   La tâche est soumise et la délégation est enregistrée.

Remarque : Les utilisateurs qui sont déjà des délégués n'apparaissent pas dans les résultats de la recherche lors de l'ajout d'un délégué.

Informations complémentaires :

Activation de la délégation (page 505)

Délégation temporelle de tâches

Dans les versions précédentes, vous pouviez spécifier l'heure de début des délégations mais pas celle de fin. Les dates des nouvelles délégations sont définies sur True, avec l'heure de début par défaut correspondant à Now (Maintenant).

Au moment de la modification, vous pouvez changer les dates de début et de fin. La date de fin par défaut correspond à une semaine après la date de début.

Pour modifier les dates de début et de fin, procédez comme suit.

1. Sous l'onglet Accueil de la console d'utilisateur, sélectionnez Gestionnaire d'absence du bureau.
2. Cliquez sur l'icône crayon en regard de l'ID de l'utilisateur dont vous souhaitez modifier les informations de délégation.

   La fenêtre Modification des détails de la délégation s'affiche.
3. Cliquez sur le calendrier à côté de la date de début pour modifier la date de début de la délégation.

   Remarque : Un message d'erreur s'affiche lorsque la date de début de la délégation sélectionnée est antérieure à la date actuelle.
4. Si vous souhaitez sélectionner une date de fin, activez la case à cocher Possède une date de fin.

   Le champ Date de fin est désormais disponible pour définir la date de fin.
5. Cliquez sur le calendrier à côté de la date de fin pour définir une date de fin pour la délégation.
6. Après avoir défini les dates, cliquez sur OK.

Vous pouvez également procéder de la sorte à partir de l'onglet Déléguer des tâches lors de la création ou de la modification d'un utilisateur.

Activation de la délégation temporelle de tâches

Pour activer la délégation temporelle de tâches dans un environnement existant lors d'une mise à niveau, procédez comme suit.

A partir de la console de gestion

1. Accédez à la page Environnements.
2. Naviguez jusqu'à l'environnement sélectionné, puis choisissez Paramètres avancés, Délégation de tâches.
3. Désactivez la case à cocher Activé.
4. Enregistrez les modifications et redémarrez l'environnement.
5. Naviguez jusqu'à Paramètres avancés et sélectionnez Délégation de tâches.
6. Activez la case à cocher Activé.
7. Enregistrez les modifications et redémarrez l'environnement.

Remarque : Cette procédure ne concerne que les environnements existants. La délégation temporelle de tâches est activée pour les nouveaux environnements.

Fenêtre du Gestionnaire d'absence du bureau

La fenêtre suivante du Gestionnaire d'absence du bureau permet d'ajouter ou supprimer des délégués personnels.

La fenêtre du Gestionnaire d'absence du bureau affiche une liste de vos délégués actuels. Outre les colonnes qui identifient le délégué, trois colonnes supplémentaires sont incluses dans la liste :

Date/heure de début

Permet d'afficher la date de création de la délégation.

Date/heure de fin

Affiche la date de fin de la délégation.

Possède des délégués

Indique si le délégué a délégué des tâches à un autre utilisateur.

Lorsque vous cliquez sur l'icône crayon en regard de l'ID d'utilisateur, la fenêtre Modifier les détails de la délégation s'affiche et vous permet de modifier la date de début et de spécifier la date de fin pour la délégation.

Délégation à un autre utilisateur

Les administrateurs peuvent déléguer des tâches d'un utilisateur (le délégateur) à un autre. Par exemple, un utilisateur peut être absent de façon imprévue ou un administrateur peut avoir besoin d'affecter une grosse tâche à plusieurs utilisateurs.

Les administrateurs peuvent uniquement déléguer les tâches des utilisateurs pour lesquels ils sont habilités. De même, ils peuvent seulement ajouter ou supprimer des utilisateurs qu'ils gèrent de la liste de délégués.

Pour déléguer des tâches d'un autre utilisateur

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, Gérer les tâches, Déléguer des tâches.

   Une fenêtre de sélection des utilisateurs apparaît.

2. Cherchez l'utilisateur dont vous souhaitez déléguer les tâches (le délégateur) et cliquez sur Sélectionner.

   Une fenêtre avec les tâches déléguées apparaît.

3. Cliquez sur Ajouter un utilisateur.

   Une fenêtre de sélection des utilisateurs apparaît.

4. Cherchez et sélectionnez un ou plusieurs utilisateurs comme délégués.

   Les utilisateurs sont ajoutés à la liste de délégués.

5. Cliquez sur Soumettre.

   La tâche est soumise et la délégation est enregistrée.

Remarque : Les utilisateurs qui sont déjà des délégués n'apparaissent pas dans les résultats de la recherche lors de l'ajout d'un délégué.

Informations complémentaires :

Activation de la délégation (page 505)

Suppression d'une délégation

Si un utilisateur se connecte à CA IdentityMinder alors qu'il a des délégations actives, CA IdentityMinder affiche le rappel suivant.

```
Vous avez des délégations actives. Vérifiez si elles sont toujours nécessaires.
```

Pour supprimer une délégation personnelle

1. Dans la console d'utilisateur, sélectionnez Accueil, Gestionnaire d'absence du bureau.

   La fenêtre du Gestionnaire d'absence du bureau apparaît.

2. Cliquez sur le signe moins (-) pour les délégués que vous souhaitez supprimer.

   Le délégué disparaît de la liste.

3. Cliquez sur Soumettre.

   La tâche est soumise et la délégation est supprimée.

Pour supprimer la délégation d'un autre utilisateur

1. Dans la console d'utilisateur, sélectionnez Utilisateurs, Gérer les tâches, Déléguer des tâches.

   Une fenêtre de sélection des utilisateurs apparaît.

2. Cherchez et sélectionnez l'utilisateur dont vous supprimer les délégations.

   La liste des délégués apparaît.

3. Cliquez sur le signe moins (-) pour les délégués que vous souhaitez supprimer.

   Le délégué disparaît de la liste.

4. Cliquez sur Soumettre.

   La tâche est soumise et la délégation est supprimée.

Remarque: Vous pouvez uniquement supprimer un délégué si vous êtes habilité pour cet utilisateur.

Réaffectation de tâches

La réaffectation permet aux utilisateurs de modifier les destinataires d'une tâche après sa création. Un administrateur peut :

- Afficher la liste de travail d'un autre utilisateur
- Ajouter et supprimer des destinataires de tâches
- Modifier l'état de réservation des tâches

Par exemple, un administrateur peut réaffecter une tâche ou libérer une tâche réservée par un utilisateur qui n'a entrepris aucune action dessus.

Si un utilisateur a réservé une tâche et qu'elle est réaffectée, il conserve cette tâche. Cependant si l'utilisateur la libère ensuite, il ne peut plus y accéder après.

Si un délégué a une tâche réservée alors que la délégation a été supprimée, il conserve l'accès jusqu'à ce que la tâche soit terminée ou libérée.

Informations complémentaires :

Réaffectation et tâches réservées (page 503)

Onglet Approbateurs

Cet onglet vous permet de réaffecter des tâches. Il contient la liste des approbateurs (ou destinataires) de tâches actuels. Lorsque vous effectuez la réaffectation, vous affectez la tâche ouverte à tous les approbateurs dans la liste. Pour réaffecter une tâche pour un nouveau destinataire, vous devez également supprimer le destinataire actuel.

Réaffectation de tâches

La réaffectation d'une tâche d'un utilisateur à un autre est un processus en deux étapes :

- Sélectionnez un nouvel approbateur.
- Supprimez l'approbateur actuel.

Remarque : Vous devez être habilité pour les utilisateurs à qui vous souhaitez réaffecter des tâches.

Réaffectation d'une tâche pour vous-même

1. Sélectionnez Accueil, Afficher ma liste de travail.

   Votre liste de travail apparaît.
2. Sélectionnez une tâche pour la développer.
3. Cliquez sur l'onglet Approbateurs.

   La liste de tous les approbateurs actuels apparaît, y compris l'utilisateur dont vous gérez la liste.
4. Cliquez sur Ajouter des destinataires.

   Une fenêtre de sélection des utilisateurs apparaît.
5. Cherchez et sélectionnez un ou plusieurs utilisateurs à qui vous souhaitez réaffecter une tâche.
6. Cliquez sur le signe moins (-) pour vous supprimer en tant que destinataire.
7. Cliquez sur Réaffectation.

   La tâche apparaît dans les listes de travail des utilisateurs réaffectés.

Remarque : Un administrateur peut réaffecter, réserver ou libérer la tâche d'un autre utilisateur mais il ne peut pas approuver ou rejeter la tâche d'un autre utilisateur. Seul le propriétaire de la tâche peut le faire.

Réaffectation d'une tâche à un autre utilisateur

1. Sélectionnez Utilisateurs, Gérer les tâches, Gérer les tâches de l'utilisateur.

   Une fenêtre de sélection des utilisateurs apparaît.

2. Cherchez l'utilisateur dont vous souhaitez réaffecter les tâches et cliquez sur Sélectionner.

   La fenêtre Gérer les tâches de l'utilisateur apparaît..

3. Sélectionnez une tâche pour la développer.

4. Cliquez sur l'onglet Approbateurs.

   La liste de tous les approbateurs actuels apparaît, y compris l'utilisateur dont vous gérez la liste.

5. Cliquez sur Ajouter des destinataires.

   Une fenêtre de sélection des utilisateurs apparaît.

6. Cherchez et sélectionnez un ou plusieurs utilisateurs à qui vous souhaitez réaffecter une tâche.

7. Cliquez sur le signe moins (-) pour supprimer le destinataire actuel.

8. Cliquez sur Réaffectation.

   La tâche apparaît dans les listes de travail des utilisateurs réaffectés.

Opérations en bloc sur les tâches

Dans cette version de CA IdentityMinder, vous pouvez effectuer les opérations en bloc suivantes sur des tâches sélectionnées.

- Approuver
- Rejeter
- Réserver
- Libérer

Dans la console d'utilisateur, l'onglet de configuration de liste de travail a été amélioré pour inclure une nouvelle case à cocher Prise en charge des opérations de flux de travaux en bloc. Lorsque cette case à cocher est activée, l'utilisateur peut approuver, rejeter, libérer et réserver en bloc des tâches dont il est le propriétaire ou des tâches provenant des délégants. Les administrateurs peuvent uniquement effectuer ces opérations en bloc sur des tâches à l'aide de la tâche Gérer les tâches de l'utilisateur.

Remarque : Vous ne pouvez pas activer d'opérations en bloc pour des tâches d'affichage, telles que Afficher ma liste de tâches.

Configuration de l'onglet Liste de travail pour les opérations en bloc

Pour configurer l'onglet Liste de travail afin de prendre en charge les opérations en bloc au niveau tâche, procédez comme suit.

Dans l'onglet Rôles et tâches de la console d'utilisateur

1. Sélectionnez Gérer les tâches, Modifier les tâches d'administration, puis cliquez sur Rechercher.
2. Sélectionnez Gérer les tâches de l'utilisateur.
3. Dans l'onglet Onglets, cliquez sur l'icône crayon en regard de Liste de travail.

   La fenêtre de configuration de la liste de travail s'affiche.
4. Sélectionnez Prise en charge des opérations de flux de travaux en bloc.

   Les opérations en bloc au niveau tâche sont désormais disponibles.

Chapitre 19: Notifications par courriel

Ce chapitre traite des sujets suivants :

Notifications par courriel dans CA IdentityMinder

Les notifications par courriel informent les utilisateurs de CA IdentityMinder des tâches et événements intervenant dans le système. Par exemple, CA IdentityMinder peut envoyer un courriel à des approbateurs lorsqu'un événement ou une tâche nécessite une approbation.

CA IdentityMinder propose deux méthodes de configuration des notifications par courriel :

- **Stratégies de notification par courriel**

  Les stratégies de notification par courriel permettent aux administrateurs de créer, consulter, modifier et supprimer des notifications par courriel par le biais de tâches dans la console d'utilisateur. La création de notifications par courriel ne nécessite aucun codage.

  Les administrateurs peuvent définir le contenu du message, le moment de son envoi et son destinataire. Le courriel peut contenir des informations dynamiques, telles que la date actuelle ou des informations sur un événement, définies dans un éditeur HTML, que CA IdentityMinder remplit lors de l'envoi du courriel. Par exemple, vous pouvez configurer une notification par courriel à envoyer à un approbateur en cas de création d'un utilisateur. Le message peut contenir les informations de connexion de l'utilisateur, sa date d'embauche et son supérieur.

  Remarque : Les stratégies de notification par courriel sont des stratégies Policy Xpress (page 329) créées et gérées par un ensemble distinct de tâches.

- **Modèles de courriel**

  Les notifications par courriel sont, dans ce cas, générées à partir de modèles de courriel. CA IdentityMinder fournit des modèles de courriel par défaut qui peuvent être utilisés en l'état ou personnalisés par les administrateurs système. Ces derniers utilisent une API de modèle de courriel pour spécifier du contenu dynamique, comme la liste des destinataires, et des informations sur l'événement qui déclenche le courriel.

CA IdentityMinder peut générer des notifications par courriel dans les cas suivants.

- Un événement nécessitant une approbation ou un rejet par un approbateur de flux de travaux est en attente.

  Remarque : Si vous avez un processus d'approbation WorkPoint qui comporte plusieurs activités d'approbation, la notification par courriel configurée dans les tâches de la console d'utilisateur envoie une notification pour chaque activité. En revanche, si vous utilisez des modèles de courriel pour la même notification, un seul courriel sera envoyé aux approbateurs (lorsque l'événement atteindra l'état En attente).

- Un approbateur approuve un événement ou une tâche.

- Un approbateur rejette un événement ou une tâche.

- Un événement ou une tâche commence, échoue ou se termine.
- Un utilisateur est créé ou modifié.

Pour utiliser des notifications par courriel CA IdentityMinder, configurez les paramètres SMTP (page 518). Si vous utilisez la méthode des modèles de courriel, vous activez également les notifications par courriel dans CA IdentityMinder.

Sélection d'une méthode de notification par courriel

Le tableau suivant résume les différences entre les stratégies de notification par courriel et les modèles de courriel :

<table>
<tr><th>Activité</th><th>Tâches de gestion de courriels</th><th>Modèles de courriel</th></tr>
<tr><td>Configuration des notifications par courriel</td><td>Les administrateurs utilisent des tâches d'administration dans la console d'utilisateur pour créer, modifier, afficher et supprimer des notifications par courriel.</td><td>Les administrateurs modifient les modèles par défaut dans les outils d'administration CA IdentityMinder.</td></tr>
<tr><td>Configuration lors de l'envoie des courriels</td><td colspan="2">CA IdentityMinder peut générer des notifications par courriel lorsque certains événements ou certaines tâches se produisent. Les tâches de gestion de courriels et les modèles de courriel prennent en charge les mêmes événements et les mêmes tâches ; toutefois, les tâches de gestion de courriels fournissent davantage de précision dans certains cas.
Les notifications par courriel sont prises en charge pour les tâches et événements suivants :
■ Un événement nécessitant une approbation ou un rejet par un approbateur de flux de travaux est en attente.
■ Remarque : Si vous avez un processus d'approbation WorkPoint qui comporte plusieurs activités d'approbation, la notification par courriel configurée à l'aide des tâches de gestion de courriels envoie une notification pour chaque activité. En revanche, si vous utilisez des modèles de courriel pour la même notification, un seul courriel sera envoyé aux approbateurs (lorsque l'événement atteindra l'état En attente).
■ Un approbateur approuve un événement ou une tâche.
■ Un approbateur rejette un événement ou une tâche.
■ Un événement ou une tâche commence, échoue ou se termine.
■ Un utilisateur est créé ou modifié.</td></tr>
</table>

Activité	Tâches de gestion de courriels	Modèles de courriel
Ajout de contenu dynamique à des courriels	Les administrateurs ajoutent le contenu dynamique au corps d'un courriel en effectuant une sélection dans une liste d'options dans l'onglet Contenu des tâches Créer un courriel ou Modifier un courriel. CA IdentityMinder remplit automatiquement le contenu dynamique en fonction des informations sur la tâche ou sur l'événement qui déclenche la notification.	Les administrateurs utilisent l'API de modèle de courriel pour personnaliser les modèles de courriel par défaut, utilisés pour générer des notifications par courriel.
Prise en charge des notifications par courriel existantes	Les notifications par courriel configurées à l'aide des tâches de gestion de courriel sont basées sur des stratégies Policy Xpress. Si vous avez effectué une mise à niveau de l'Option Pack 1 CA IdentityMinder vers CA IdentityMinder r12.6.1, les notifications par courriel configurées dans Policy Xpress continueront de fonctionner. Toutefois, gérez ces notifications par courriel à l'aide des tâches de gestion de courriels, au lieu d'utiliser Policy Xpress.	Les notifications par courriel créées à l'aide de la méthode de modèle de courriel des versions précédentes de CA IdentityMinder continueront de fonctionner dans CA IdentityMinder r12.6.1.

Configuration des paramètres SMTP

Avant d'activer les notifications par courriel, configurez les paramètres SMTP. Pour configurer les paramètres SMTP pour votre serveur d'applications, consultez les sections suivantes.

Configuration des paramètres SMTP sous JBoss

1. Dans un éditeur de texte, ouvrez le descripteur de déploiement de service de messagerie comme suit :

   Noeud unique : *jboss_home*\server\default\deploy\mail-service.xml

   Cluster : *jboss_home*\server\all\deploy\mail-service.xml

2. Modifiez la propriété mail.smtp.host avec le nom de votre serveur SMTP comme suit :

   ```
   <-- Changement du serveur de passerelle SMTP -->
   <nom propriété"mail.smtp.host" valeur="votre_serveur_smtp/>
   ```

   Exemple :

   ```
   <nom propriété="mail.smtp.host" valeur="smtp.mailserver.company.com"/>
   ```

3. Enregistrez le fichier mail-service.xml.

4. Dans un éditeur de texte, ouvrez le fichier de propriétés de courriel suivant :

   Noeud unique :
   jboss_home\server\default\deploy\iam_im.ear\config\com\netegrity\config\email.properties

   Cluster
   :*jboss_home*\server\all\farm\iam_im.ear\config\com\netegrity\config\email.properties

5. Pour définir l'adresse de l'expéditeur de courriel utilisée par le courriel généré par le flux de travaux, recherchez la propriété admin.email.address et définissez la valeur sur l'adresse électronique appropriée. Exemple :

   ```
   admin.email.address=admin@company.com
   ```

6. Si vous utilisez la méthode des modèles de courriel, activez les notifications par courriel dans la console de gestion.

   Il n'est pas nécessaire d'activer des notifications par courriel dans la console de gestion si vous utilisez des stratégies de notification par courriel.

Configuration des paramètres SMTP sous WebLogic

Configurez des paramètres de messagerie dans la console d'administration de serveur WebLogic et dans un fichier email.properties.

Pour configurer les paramètres de courriel pour WebLogic :

1. Dans la console d'administration de serveur WebLogic, créez une session de courriel avec les propriétés suivantes :

   - Propriété **mail.smtp.host** : définissez cette valeur sur votre serveur SMTP. Par exemple : mail.smtp.host=mymailserver.company.com
   - Propriété **mail.transport.protocol** : définissez cette valeur sur SMTP. Par exemple : mail.transport.protocol=smtp
   - **Nom JNDI** : nete/Mail
   - **Cible** : saisissez le nom du serveur WebLogic.

2. Dans un éditeur de texte, ouvrez le fichier de propriétés de courriel suivant pour CA IdentityMinder :

   weblogic_domain\applications\iam.ear\config\com\netegrity\config\email.properties

3. Définissez l'adresse de l'expéditeur utilisée par les courriels générés par le flux de travaux en recherchant la propriété admin.email.address et en définissant la valeur sur l'adresse électronique appropriée. Exemple :

   `admin.email.address=admin@company.com`

4. Activez la notification par courriel dans la console de gestion.

   Remarque : Il n'est pas nécessaire d'activer des notifications par courriel dans la console de gestion si vous utilisez des stratégies de notification par courriel.

Configuration des paramètres SMTP sous WebSphere

L'utilitaire imsSetup que vous exécutez après l'installation des composants CA IdentityMinder configure un nouvel objet de session de courriel appelé mailMail.

Pour le fonctionnement correct de la fonctionnalité de notification par courriel, spécifiez le serveur auquel WebSphere se connecte lors de l'envoie de courriel dans le champ Mail Transport Host (Hôte de transport de courriel) pour la session mailMail.

La session mailMail se trouve sous Ressources, Mail Providers (Fournisseurs de courriels), Built-in Mail Provider (Fournisseur de courriels intégrés), Mail Sessions (Sessions de courriel), mailMail dans la console d'administration de WebSphere.

Remarque : Pour afficher l'objet mailMail, modifiez la portée sur Server dans la fenêtre Mail sessions (Sessions de courriel). Sans quoi, l'objet mailMail ne s'affichera pas.

Pour plus d'informations sur la configuration d'un fournisseur de courriel WebSphere, consultez la documentation de WebSphere.

Si vous utilisez la méthode de modèle de courriel, activez la notification par courriel dans la console de gestion une fois les paramètres SMTP configurés.

Remarque : Il n'est pas nécessaire d'activer des notifications par courriel dans la console de gestion si vous utilisez des stratégies de notification par courriel.

Création de stratégies de notification par courriel

La console d'utilisateur permet de créer des stratégies de notification par courriel qui envoient des messages électroniques lorsque certaines actions ont lieu. Par exemple, vous pouvez créer une stratégie de notification par courriel qui envoie un message pour informer les approbateurs en cas de création d'un utilisateur.

Pour créer une stratégie de notification par courriel

1. Sous l'onglet Système, sélectionnez Courriel, Créer un courriel.
2. Sélectionnez l'une des options suivantes.
   - Créer un objet de type Courriel géré

     Crée une nouvelle stratégie de notification par courriel.
   - Créer une copie d'objet de type Courriel géré

     Utilise une stratégie de notification par courriel existante comme modèle pour en créer une nouvelle.
3. Spécifiez les informations de base de la stratégie de notification par courriel sous l'onglet Profil.
4. Indiquez à quel moment CA IdentityMinder envoie le courriel sous l'onglet Planification de l'envoi.

   Cet onglet propose diverses options qui permettent de spécifier les actions qui déclenchent les notifications par courriel.
5. Indiquez les destinataires du courriel sous l'onglet Destinataires.
6. Définissez l'objet et le contenu du courriel sous l'onglet Contenu.

   Vous pouvez spécifier, dans le contenu du courriel, des attributs d'utilisateurs ainsi que du contenu dynamique, tel que la date, la tâche ou le nom de l'événement.

Informations complémentaires :

Onglet Profil de notification par courriel (page 522)
Onglet Planification de l'envoi (page 523)
Onglet Destinataires (page 525)
Contenu (page 526)

Onglet Profil de notification par courriel

L'onglet Profil dans les tâches de gestion des courriels permet de spécifier des informations de base sur une stratégie de notification par courriel. Cet onglet contient les champs suivants.

Nom de courriel

Identifie la stratégie de notification par courriel dans la console d'utilisateur.

Remarque : Le nom du courriel n'apparaît pas lors de son envoi. Il sert uniquement à la gestion de la stratégie de notification par courriel dans la console d'utilisateur.

Catégorie

Regroupe les stratégies de notification par courriel pour en simplifier la gestion.

Vous pouvez spécifier une catégorie existante en la sélectionnant dans la liste déroulante ou activer le deuxième bouton d'option pour entrer le nom d'une nouvelle catégorie.

Description

Décrit la stratégie de notification par courriel pour les administrateurs.

La description n'apparaît pas lors de l'envoi du courriel.

Activé

Indique que CA IdentityMinder envoie le courriel lorsque les conditions définies sous l'onglet Planification de l'envoi sont remplies.

Données personnalisées

Crée un élément de données personnalisé dans Policy Xpress qui permet de configurer des destinataires ou du contenu personnalisés.

Les éléments de données personnalisés peuvent également servir de paramètres dans d'autres éléments de données.

Remarque : La section Données (page 336) fournit des informations supplémentaires sur les éléments de données.

Lorsque vous cliquez sur Données personnalisées, CA IdentityMinder ouvre une fenêtre permettant d'ajouter de nouveaux éléments de données.

Règles de saisie

Définit les règles pour que CA IdentityMinder envoie des notifications par courriel lorsque les règles par défaut de l'onglet Planification de l'envoi ne sont pas suffisamment précises.

Imaginons, par exemple, que l'onglet Planification de l'envoi comporte une règle par défaut qui envoie un courriel lorsqu'un attribut d'un profil utilisateur est modifié. Si vous souhaitez que CA IdentityMinder envoie un courriel uniquement en cas de modification du service d'un utilisateur, vous pouvez créer une règle de saisie personnalisée. Dans ce cas, vous créez un élément de données personnalisé qui détecte quand le service change, puis vous créez une règle de saisie qui utilise cet élément.

Remarque : La section Règles de saisie (page 339) fournit plus d'informations.

Onglet Planification de l'envoi

CA IdentityMinder propose plusieurs options par défaut qui déterminent à quel moment le courriel est envoyé. Certaines d'entre elles nécessitent la saisie d'informations supplémentaires, comme le nom d'une tâche ou d'un événement. Par exemple, si vous souhaitez envoyer un message lorsqu'une tâche commence, vous devez sélectionner la tâche qui déclenche ce dernier.

Vous pouvez sélectionner une ou plusieurs des options suivantes de planification d'envoi.

Utilisateur créé

Envoie un courriel en cas de création d'un utilisateur. Le message est émis une fois l'événement CreateUserEvent terminé.

Utilisateur modifié

Envoie un courriel en cas de modification d'un utilisateur. Le message est émis une fois l'événement ModifyUserEvent terminé.

Flux de travaux en attente

Envoie un courriel lorsqu'un processus de flux de travaux affecte un approbateur. Si vous sélectionnez cette option, vous devez spécifier le processus de flux de travaux concerné. Le courriel défini avec cette stratégie est un courriel envoyé à chaque approbateur à chaque étape du processus de flux de travaux sélectionné.

Courriel de flux de travaux en attente

Envoie un courriel lorsqu'un processus de flux de travaux atteint une activité spécifiée. Si vous sélectionnez cette option, vous devez spécifier le processus de flux de travaux concerné. Le courriel défini avec cette stratégie envoie un courriel de notification pour chaque étape d'approbation.

Evénement démarré

Envoie un courriel lorsqu'un événement atteint l'état Avant. Si vous sélectionnez cette option, vous devez spécifier l'événement concerné.

Remarque : Si vous spécifiez Evénement démarré et que le courriel ne soit pas envoyé, l'événement associé à la notification ne s'exécutera pas.

Evénement terminé

Envoie un courriel lorsqu'un événement atteint l'état Après. Si vous sélectionnez cette option, vous devez spécifier l'événement concerné.

Evénement approuvé

Envoie un courriel lorsqu'un événement atteint l'état Approuvé. Si vous sélectionnez cette option, vous devez spécifier l'événement concerné.

Evénement rejeté

Envoie un courriel lorsqu'un événement atteint l'état Rejeté. Si vous sélectionnez cette option, vous devez spécifier l'événement concerné.

Echec de l'événement

Envoie un courriel lorsqu'un événement échoue. Si vous sélectionnez cette option, vous devez spécifier l'événement concerné.

Tâche soumise

Envoie un courriel lorsque le traitement de la tâche commence. Si vous sélectionnez cette option, vous devez spécifier la tâche concernée.

Fin de la tâche

Envoie un courriel lorsque la tâche est terminée. Si vous sélectionnez cette option, vous devez spécifier la tâche concernée.

Echec de la tâche

Envoie un courriel si la tâche échoue. Si vous sélectionnez cette option, vous devez spécifier la tâche concernée.

Onglet Destinataires

Plusieurs destinataires peuvent être configurés pour les champs A, Cc ou Cci d'un courriel. La liste des destinataires peut être statique ou dépendre du type d'action qui déclenche le courriel et des utilisateurs concernés.

Pour spécifier les destinataires, sélectionnez l'icône Modifier en regard du champ A, Cc ou Cci de l'onglet Destinataires. Ensuite, sélectionnez l'une des options suivantes pour configurer la liste des destinataires :

Approbateurs de flux de travaux

Envoie le courriel à tous les approbateurs du processus de flux de travaux. Cette option est uniquement applicable si le courriel est envoyé pour un événement de flux de travaux en attente.

Gestionnaire

Envoie le courriel au gestionnaire de l'utilisateur sur lequel la tâche a été effectuée.

Remarque : Pour utiliser l'option de destinataire Gestionnaire, configurez l'attribut de gestionnaire de l'environnement. Pour ce faire, allez dans Environments (Environnements), *Nom_environnement*, Advanced Settings (Paramètres avancés), Miscellaneous (Divers) dans la console de gestion. Définissez managerattribute sur le nom de l'attribut physique qui contient le nom unique du gestionnaire de l'utilisateur.

Pour les bases de données relationnelles, spécifiez l'attribut au format suivant :

tablename.attribute

Membres du groupe

Envoie le courriel à tous les membres d'un groupe. La sélection de cette option ouvre une liste déroulante reprenant les noms de groupes disponibles.

Membres avec rôles

Envoie le courriel à tous les membres d'un rôle d'administration. La sélection de cette option ouvre une liste déroulante reprenant les noms de rôles disponibles.

Adresse statique

Envoie le courriel à une adresse électronique spécifique. Vous pouvez définir cette dernière dans la zone de texte supplémentaire disponible.

Remarque : Ne spécifiez qu'une seule adresse dans la zone de texte.

Utilisateur

Envoie le courriel à l'utilisateur sur lequel la tâche a été effectuée.

Auteur

Envoie le courriel à la personne ayant formulé la demande.

Personnalisé

Permet de sélectionner un élément de données personnalisé pour définir les destinataires.

La sélection de l'option Personnalisé ouvre une liste déroulante reprenant les éléments de données personnalisés disponibles.

Remarque : La section Données (page 336) fournit des informations supplémentaires sur les éléments de données.

Contenu

Vous pouvez définir l'objet et le contenu d'un courriel par le biais d'un texte simple ou par l'ajout d'un contenu dynamique calculé au moment de l'envoi du message.

La ligne de l'objet est un champ de texte brut dans lequel vous pouvez écrire votre message. Celui-ci indique l'objet du courriel.

Le corps du message s'affiche dans un éditeur HTML. Vous pouvez insérer n'importe quel texte et le mettre en forme pour constituer le corps du courriel.

Pour y inclure du contenu dynamique, vous devez sélectionner des options dans une liste déroulante. L'éditeur ajoute alors, à l'emplacement du curseur, des indicateurs de contenu dynamique semblables au suivant.

{*type*}

type représente l'un des types de contenu dynamique pris en charge.

Par exemple, si vous sélectionnez le type de contenu dynamique Attribut et spécifiez l'attribut Prénom, l'éditeur HTML affiche ce qui suit sous l'onglet Contenu.

{'Attribut: Prénom'}

Remarque : Pour ajouter du contenu dynamique dans la ligne de l'objet, utilisez la liste déroulante en dessous de celle-ci. Pour ajouter du contenu dynamique dans le corps du courriel, utilisez la liste déroulante en dessous de la zone du contenu.

A l'envoi du courriel, CA IdentityMinder remplace le contenu dynamique par le texte approprié. Le texte conserve la mise en forme (caractères en gras, surlignés, etc.) spécifiée dans l'éditeur HTML.

Les types de contenu dynamique sont les suivants.

Date

Indique la date du jour au format spécifié.

Tâche

Indique la tâche pour laquelle le courriel est envoyé.

Nom de l'objet

Indique le nom de l'objet dans l'événement qui déclenche le courriel. S'il s'agit d'un événement utilisateur, ce champ correspond au nom de connexion de l'utilisateur.

Ce peut toutefois être autre chose qu'un objet Utilisateur. Il peut, par exemple, être question de n'importe quel objet géré, comme un groupe, un rôle d'administration, etc.

Attribut

Indique la valeur de l'un des attributs d'utilisateur. L'utilisateur est le sujet de la tâche. Cette option implique de sélectionner l'attribut à partir d'une liste déroulante.

Attribut Gestionnaire

Indique la valeur de l'un des attributs du gestionnaire de l'utilisateur. L'utilisateur est le sujet de la tâche. Cette option implique de sélectionner l'attribut à partir d'une liste déroulante.

Remarque : Pour utiliser l'option de destinataire Gestionnaire, configurez l'attribut de gestionnaire de l'environnement. Pour ce faire, allez dans Environments (Environnements), *Nom_environnement*, Advanced Settings (Paramètres avancés), Miscellaneous (Divers) dans la console de gestion. Définissez managerattribute sur le nom de l'attribut physique qui contient le nom unique du gestionnaire de l'utilisateur.

Pour les bases de données relationnelles, spécifiez l'attribut au format suivant :

tablename.attribute

Personnalisé

Permet de sélectionner un élément de données personnalisé pour définir les destinataires.

La sélection de l'option Personnalisé ouvre une liste déroulante reprenant les éléments de données personnalisés disponibles.

Remarque : La section Données (page 336) fournit des informations supplémentaires sur les éléments de données.

Modification des stratégies de notification par courriel

Une stratégie existante de notification par courriel peut être modifiée pour l'adapter à vos besoins métiers.

Pour modifier une stratégie de notification par courriel

1. Allez dans Système, Courriel, Modifier un courriel.

   CA IdentityMinder affiche une fenêtre de recherche.

2. Recherchez la stratégie de notification par courriel à modifier et sélectionnez-la.
3. Modifiez les paramètres sous les onglets Profil, Planification de l'envoi, Destinataires et Contenu comme requis.

Désactivation des stratégies de notification par courriel

Les stratégies de notification par courriel peuvent être activées ou désactivées par le biais de la case à cocher Activé sous l'onglet Profil lors de leur création ou de leur modification. Si une stratégie de notification par courriel est désactivée, le message sélectionné est inactif et n'est pas envoyé.

Remarque : Les nouvelles stratégies de notification par courriel sont activées par défaut.

Cas d'utilisation : Envoi d'un courriel de bienvenue

Lorsqu'elle engage un nouvel employé, la société Forward souhaite lui envoyer un courriel pour lui souhaiter la bienvenue. Ce message doit contenir des informations importantes pour ce nouvel utilisateur, telles que des liens vers la page d'accueil de ce dernier, ainsi que des renseignements sur son supérieur et son service.

Pour créer le courriel, l'administrateur des Ressources humaines utilise la tâche Créer un courriel de la console d'utilisateur pour configurer les paramètres suivants.

- Sous l'onglet Planification de l'envoi, sélectionnez Utilisateur créé.
- Sous l'onglet Destinataires, effectuez les étapes ci-dessous.
  - Cliquez sur l'icône Modifier située en regard du champ A.

    Sélectionnez Utilisateur, puis cliquez sur le signe plus. Sélectionnez le gestionnaire (autrement dit, le supérieur) de la même manière, puis cliquez sur OK.
  - Cliquez sur l'icône Modifier située en regard du champ Cc.

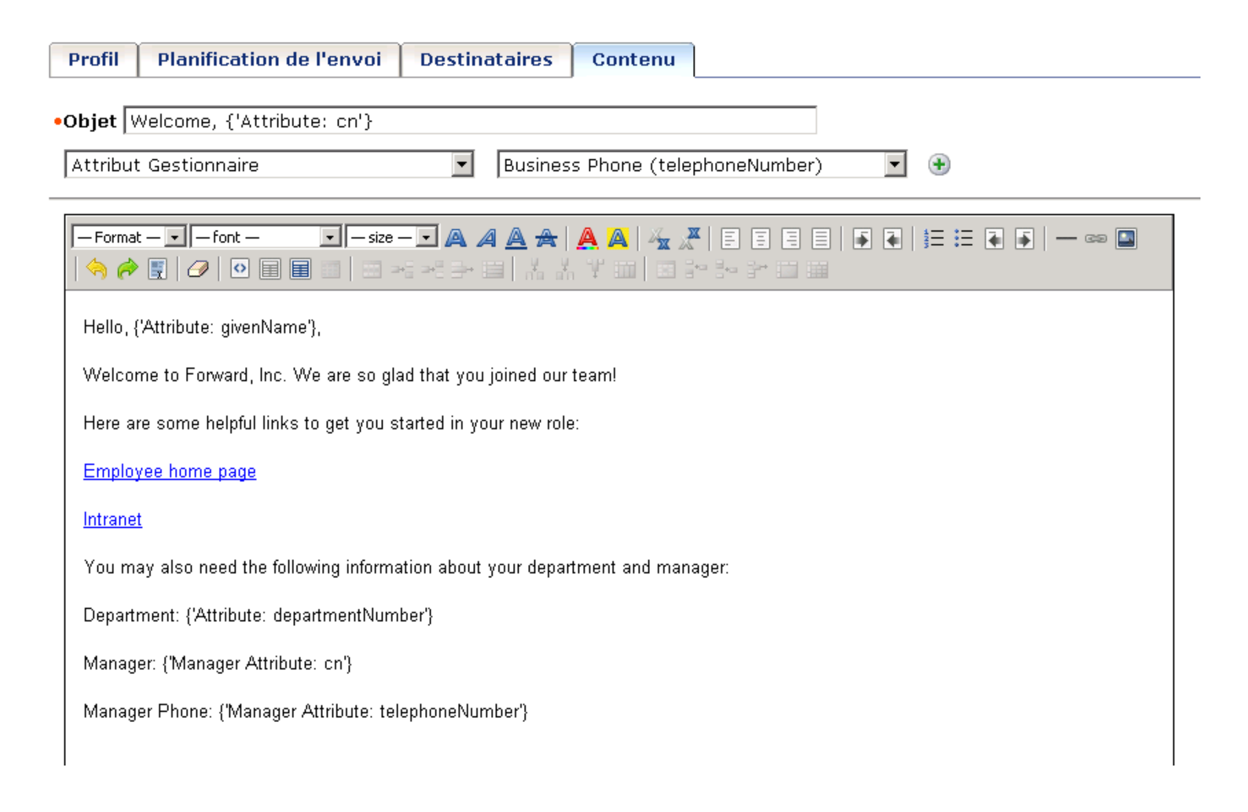
    Sélectionnez Auteur et cliquez sur le signe plus, puis sur OK pour envoyer une copie du courriel à l'utilisateur ayant créé l'employé dans CA IdentityMinder.
- Sous l'onglet Contenu, effectuez les étapes ci-dessous.
  - Dans le champ Objet, entrez le texte "Bienvenue,".

    Tandis que le curseur se situe à la fin du texte que vous venez d'entrer, sélectionnez Attribut dans la liste déroulante. Sélectionnez ensuite Nom complet dans la deuxième liste déroulante, puis cliquez sur le signe plus.

    La ligne de l'objet ressemble à ceci :

    Bienvenue, {'Attribut: eTNomComplet'}

    Remarque : Le nom de l'attribut dépend du magasin d'utilisateurs et de l'attribut que vous utilisez.
  - Dans la zone Contenu, ajoutez le texte de bienvenue souhaité. Insérez-y des liens vers le portail Employé et utilisez les options de contenu dynamique en dessous de la zone de contenu pour afficher le service de l'utilisateur, ainsi que son supérieur avec son numéro de téléphone, comme illustré ci-dessous.



Utilisation des modèles de courriel

CA IdentityMinder inclut des modèles de courriel par défaut que vous pouvez utiliser pour générer des courriels. Vous pouvez utiliser ces modèles par défaut tels quels ou les personnaliser selon vos besoins.

Pour utiliser des modèles de courriel :

1. Configurez les paramètres SMTP de sorte à permettre à CA IdentityMinder d'envoyer des notifications par courriel.
2. Activez la notification par courriel dans la console de gestion (page 531).
3. Configurez un événement ou une tâche à envoyer par courriel (page 531)
4. (Facultatif) Personnalisez les modèles par défaut (page 537), si nécessaire.

Activation de la notification par courriel

Vous pouvez activer ou désactiver la notification par courriel pour un environnement CA IdentityMinder. Si vous activez les notifications par courriel, CA IdentityMinder envoie des notifications par courriel pour des événements et des tâches que vous spécifiez.

Remarque : Pour utiliser la fonctionnalité Mot de passe oublié, activez la notification par courriel.

Avant d'activer les notifications par courriel dans CA IdentityMinder, configurez les paramètres SMTP (page 518) de votre serveur d'applications.

Pour activer la notification par courriel :

1. Dans la console de gestion, cliquez sur Environnements.

   Une liste d'environnements CA IdentityMinder s'affiche.

2. Cliquez sur l'environnement CA Identity Manager approprié.
3. Accédez à Paramètres avancés, Courriel.
4. Sélectionnez la case à cocher Activé.
5. Configurez les événements et les tâches qui déclenchent l'envoi d'un courriel (page 531).
6. Cliquez sur Enregistrer.
7. Redémarrez l'instance du serveur d'applications sur lequel CA IdentityMinder est installé.

Configuration d'un événement ou d'une tâche à envoyer par courriel

Si la notification par courriel est activée, vous pouvez spécifier une liste d'événements et de tâches qui déclenchent des notifications par courriel. Par exemple, vous pouvez décider d'envoyer un courriel dans les cas suivants :

- A un administrateur système, à l'issue d'une tâche de réinitialisation de mot de passe d'un utilisateur
- Au gestionnaire d'un nouvel employé, à l'issue d'une tâche Créer un utilisateur. De plus, lorsque l'événement AddToGroupEvent généré dans la tâche Créer un utilisateur est approuvé, vous pouvez envoyer un autre courriel à tous les membres d'un groupe auquel le nouvel utilisateur est ajouté.

Pour spécifier des événements et des tâches qui déclenchent des notifications par courriel :

1. Dans la console de gestion, cliquez sur Environnements.

   Une liste d'environnements CA IdentityMinder s'affiche.

2. Cliquez sur l'environnement CA IdentityMinder approprié.

3. Accédez à Paramètres avancés, Courriel.

   La fenêtre Email Properties (Propriétés de courriel) s'ouvre.

4. Sélectionnez les cases à cocher Activer suivantes qui s'appliquent :

   - Events E-mail Enabled (Activation de courriel pour des événements)

     Active la notification par courriel pour des événements CA IdentityMinder.

   - Tasks Email Enabled (Activation de courriel pour des tâches)

     Active la notification par courriel pour des tâches CA IdentityMinder.

5. Saisissez l'emplacement des modèles de courriel que CA IdentityMinder utilise pour la création des courriels.

   Les modèles de courriel se trouvent dans un sous-répertoire à l'emplacement suivant :

   iam_im.ear\custom\emailTemplates

   Remarque : Lors de la création d'un fichier de modèle de courriel portant un nom utilisant une langue différente, la session du système d'exploitation doit fonctionner dans une langue qui prend en charge le jeu de caractères.

6. Spécifiez les événements pour lesquels les notifications par courriel sont envoyées comme suit :

   - Pour ajouter un événement, sélectionnez-le dans la zone de Liste Evénements et cliquez sur Ajouter.

     CA IdentityMinder ajoute l'événement sélectionné à la liste d'événements pour lesquels des notifications par courriel sont envoyées.

     Remarque : Si vous sélectionnez un événement non associé à un processus de flux de travaux, CA IdentityMinder envoie une notification par courriel à l'issue de l'événement.

   - Pour supprimer un événement, sélectionnez la case à cocher de l'événement, puis cliquez sur Supprimer.

7. Spécifiez les tâches pour lesquels les notifications par courriel sont envoyées comme suit :

   - Pour ajouter une tâche, recherchez-la en sélectionnant une condition dans le premier champ, puis saisissez un nom de tâche dans le deuxième champ. Cliquez sur Rechercher.

     Vous pouvez saisir un nom de tâche partiel à l'aide du caractère générique (*). Par exemple, pour rechercher une tâche Créer, saisissez Create*.

     Sélectionnez une ou plusieurs des tâches parmi les résultats de la recherche. Cliquez sur Ajouter.

     Remarque : Les notifications par courriel de niveau tâche ne sont pas disponibles pour des tâches contenant le type d'action Affichage ou Auto-affichage. Pour afficher le type d'action d'une tâche, accédez à Modifier la tâche d'administration, Sélectionner une tâche et vérifiez le champ d'action dans le profil de la tâche.

   - Pour supprimer une tâche, sélectionnez la case à cocher de la tâche, puis cliquez sur Supprimer.

     Cela supprime la tâche de la table Tâche, mais ne supprime pas la tâche.

8. A l'issue de la configuration des tâches et des événements qui déclenchent des notifications par courriel, cliquez sur Enregistrer.

9. Redémarrez le serveur d'applications sur lequel CA IdentityMinder est installé.

Contenu de courriel

Les notifications par courriel contiennent un modèle générique et des détails spécifiques sur les tâche, ajoutés au courriel à travers l'API de messagerie. Par exemple, vous pouvez insérer les informations suivantes dans un courriel pour une tâche Créer un utilisateur :

- Le nom de l'administrateur qui exécute la tâche
- Le nom du nouvel utilisateur
- L'adresse électronique de l'utilisateur, le nom du service et autres données d'attribut
- L'organisation dans laquelle l'utilisateur est créé
- Statut d'approbation de flux de travaux et heure d'approbation
- Le nom de tâche et les noms des événements dans la tâche

Modèles de courriel

Les notifications par courriel sont générées à partir de modèles de courriel. CA Identity Manager fournit des modèles de courriel par défaut que vous pouvez utiliser une fois installé, ou que vous pouvez utiliser pour créer vos propres modèles de courriel.

Chaque modèle de courriel contient les éléments suivants :

- **Informations de remise**: liste des destinataires du courriel. CA Identity Manager génère automatiquement la liste des destinataires, en fonction des utilisateurs concernés par la tâche. Par exemple, un courriel d'approbation est envoyé à tous les approbateurs de la tâche.
- **Objet :** texte utilisé dans la ligne d'objet du message
- **Contenu** : corps du message. En général, le corps contient du texte statique et des variables, que CA Identity Manager résout en fonction de la tâche ou de l'événement qui déclenche le courriel.

Les modèles de courriel par défaut se trouvent dans un répertoire emailTemplates dans lequel les outils d'administration de CA Identity Manager sont installés. L'emplacement d'installation par défaut des outils d'administration est le suivant :

- Sous Windows : C:\Program Files\CA\CA Identity Manager\
- Sous UNIX : <home_directory>/CA/CA Identity Manager

Le répertoire emailTemplates contient quatre dossiers. Chaque dossier est associé à un état de tâche ou d'événement :

Annuaire	Sommaire
Approuvé	defaultEvent.tmpl : informe les destinataires qu'un événement a été approuvé.

Annuaire	Sommaire
Terminé	■ CertificationNonCertifiedActionCompletedNotification.tmpl : informe le gestionnaire qu'une action de non-conformité a été appliquée à un employé. ■ CertificationNonCertifiedActionPendingNotification.tmpl : informe le gestionnaire qu'une action de non-conformité sera appliquée à un employé. ■ CertificationRequiredFinalNotification.tmpl : dernier rappel indiquant à un gestionnaire que la tâche Certifier un utilisateur doit être effectuée pour un employé. ■ CertificationRequiredNotification.tmpl : informe le gestionnaire qu'un processus de certification a démarré pour un employé. Le gestionnaire doit réaliser une tâche Certifier un utilisateur pour cet employé. ■ CertificationRequiredReminderNotification.tmpl : rappelle au gestionnaire que la tâche Certifier un utilisateur doit être effectuée pour un employé. ■ Certify Employee.tmpl : informe un administrateur que le processus de certification pour un employé est terminé. ■ CreateProvisioningUserNotificationEvent.tmpl : envoie un mot de passe temporaire à un utilisateur lorsque son compte est créé dans l'annuaire de provisionnement. ■ defaultTask.tmpl : informe les destinataires que CA Identity Manager a terminé une tâche. ■ ForgottenPassword.tmpl : envoie un mot de passe temporaire aux utilisateurs qui ont utilisé la fonctionnalité de mot de passe oublié. ■ ForgottenUserID.tmpl : envoie un ID d'utilisateur aux utilisateurs qui ont utilisé la fonctionnalité d'ID d'utilisateur oublié. ■ Self Registration.tmpl : informe un utilisateur qu'une tâche d'auto-enregistrement s'est correctement terminée.
En attente	■ defaultEvent.tmpl : informe les approbateurs qu'un élément de liste de travail nécessite une attention. ■ ModifyUserEvent.tmpl : identique au modèle par défaut, mais inclut des méthodes de récupération des attributs de l'objet géré par l'utilisateur.
Rejeté	defaultEvent.tmpl : informe les destinataires qu'un événement a été rejeté.

Utilisez les modèles CA Identity Manager et la structure de répertoires de modèle qui sont installés sous le répertoire emailTemplates <*rép_outils_admin_im*>\Identity Manager\
comme base pour la création des modèles de courriel personnalisés.

Répertoires de modèles

Chaque répertoire de modèles décrit sous la section Modèles de courriel (page 534) est associé à un état de tâche ou d'événement particulier. Par exemple, si un courriel doit être envoyé pour un événement rejeté dans un processus de flux de travaux, CA Identity Manager recherche le modèle à utiliser dans un répertoire de modèles rejetés déployés. CA Identity Manager génère ensuite le courriel à partir du modèle de courriel approprié dans le répertoire.

Modèles de courriel dans un répertoire

Chaque répertoire de modèles déployés contient un ou plusieurs modèles de courriel. Lorsqu'une tâche ou un événement pour lequel un courriel est activé se produit, CA Identity Manager recherche dans le répertoire de modèles approprié un nom de modèle identique à celui de la tâche ou de l'événement. Si ce modèle est introuvable, CA Identity Manager utilise le modèle par défaut dans le répertoire. Les noms de modèle par défaut sont répertoriés sous Modèles de courriel (page 534). Par exemple, CA Identity Manager utilise defaultEvent.tmpl dans le répertoire En attente pour informer les approbateurs qu'un nouvel élément de liste de travail est disponible.

Ensembles de répertoires de modèles

Un ensemble de répertoires de modèles contient un répertoire approuvé, un répertoire terminé, un répertoire en attente et un répertoire rejeté. Vous pouvez déployer plusieurs ensembles de répertoires de modèles et spécifier un ensemble à utiliser pour un environnement CA Identity Manager particulier.

Le déploiement de modèle de courriel (page 556)fournit des informations sur le déploiement d'ensembles de répertoires de modèle.

Pour plus d'informations sur la configuration des répertoires de modèle de courriel de sorte que CA Identity Manager utilise l'ensemble correct pour un environnement donné, consultez le *Manuel de configuration de CA Identity Manager*.

Création de modèles de courriel

Pour créer des courriels personnalisés :

1. Ouvrez le modèle que vous voulez modifier.

   Par exemple, si vous voulez créer un courriel pour un événement en attente Créer un utilisateur, ouvrez defaultEvent.tmpl dans le répertoire En attente.

2. Enregistrez le modèle dans le même répertoire sous un nouveau nom. Ce nom doit correspondre au nom de l'événement auquel le courriel s'applique et portez l'extension .tmpl.

   Par exemple, nommez le message pour l'événement en attente Créer un utilisateur comme suit :

   CreateUserEvent.tmpl

   Pour obtenir une liste d'événements, consultez la section Evénements CA Identity Manager.

   Remarque : Lors de la création d'un fichier de modèle de courriel portant un nom utilisant une langue différente, la session du système d'exploitation doit fonctionner dans une langue qui prend en charge le jeu de caractères.

3. Modifiez le modèle de message en fonction de vos besoins, tel que décrit dans la section suivante, Modèles de courriel personnalisés (page 537).

Modèles de courriel personnalisés

Un modèle de courriel est un fichier dynamique qui prend en charge HTML et JavaScript intégré côté serveur. Un modèle permet d'insérer des valeurs variables dans un texte statique, autorisant la génération de messages spécifiques à partir d'un modèle unique.

Vous pouvez utiliser le même modèle autant de fois que vous voulez pour imprimer le texte statique réutilisable (par exemple : la phrase a été approuvée) avec du texte variable spécifique à un contexte donné (tel que le nom de l'événement en cours d'approbation).

Voici un exemple de modèle signalant l'approbation d'un événement :

```
<!-- Define the E-mail Properties --->
<%
   _to = _util.getNotifiers("ADMIN");
   _cc = "" ;
   _bcc = "";
   _subject = _eventContextInformation.getEventName() + " approved";
%>
<!--- Start of Body --->
<html>
<body text="Navy">
```

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
Status: <b>Approved</b>
</body>
</html>
```

Remarque : Les objets CA Identity Manager _util et _eventContextInformation utilisés dans l'exemple ci-dessus sont décrits dans l'API de modèle de courriel.

Si une approbation est générée pour l'événement CreateUserEvent et que l'utilisateur John Jones est créé dans l'organisation RH, le corps de la notification par courriel générée à partir du modèle d'approbation serait similaire à l'exemple suivant :

```
Event: CreateUserEvent
USER: John Jones
In ORGANIZATION: HR
Status: Approved
```

Les sections suivantes décrivent la syntaxe et les objets CA Identity Manager qui permettent la création de courriels dynamiques.

Eléments de modèle

Les modèles de courriel CA Identity Manager prennent en charge les éléments suivants :

- Balises HTML standard
- JavaScript côté serveur
- Un ou plusieurs objets implicites mis à la disposition par CA Identity Manager à une instance du modèle, c'est-à-dire à un courriel.
- Balises CA Identity qui permettent d'intégrer JavaScript dans le modèle, d'appeler les méthodes dans les objets CA Identity Manager implicites et d'insérer des valeurs variables dans le texte statique du modèle

Extensions de balise Identity Manager

Les modèles de courriel prennent en charge les balises suivantes :

<% %>

Intègre JavaScript dans un modèle de courriel.

<%= %>

Insère une valeur variable dans le texte statique.

Les balises sont décrites dans les sections suivantes.

<% %>

Cette balise permet d'intégrer JavaScript pour une exécution en ligne dans un modèle de courriel.

Vous pouvez utiliser un objet JavaScript dans JavaScript intégré. Vous pouvez également appeler des méthodes d'objet CA Identity Manager implicite dans JavaScript intégré.

Par exemple, le code suivant modifie le corps du modèle d'approbation affiché dans les modèles de courriel personnalisés (page 537). JavaScript est utilisé pour déterminer si un objet secondaire est concerné par l'événement (tel qu'un objet ORGANISATION lorsqu'un objet principal UTILISATEUR est ajouté). Si aucun objet secondaire n'existe, le texte relatif à l'objet secondaire sera retiré du message :

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType =       _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                              ObjectName()+" </b><br>");
   }
%>
Status: <b>Approved</b>
```

<%= %>

Cette balise permet d'insérer une valeur variable dans du texte statique. La valeur peut être la suivante :

- Une variable définie dans un JavaScript préalablement exécuté dans le modèle. Par exemple :

```
<%
var secondaryType
=      _eventContextInformation.getSecondaryObjectTypeName();
...          // More JavaScript processing
%>
...          // More HTML
The primary object was created in <%=secondaryType%>.
```

- Une valeur est renvoyée à partir d'une méthode dans un objet CA Identity Manager implicite. Par exemple :

```
Event <%=_eventContextInformation.getEventName()%> is approved.
```

API de modèle de courriel

Lorsqu'un message est généré à partir d'un modèle, CA Identity Manager rend les objets implicites placés dessous disponibles pour le message. Ces objets permettent d'insérer des informations spécifiques à l'instance dans un message en appelant des méthodes dans l'API de modèle de courriel.

Un modèle peut appeler les méthodes dans les objets suivants :

- _contentType. Spécifie le type de contenu du courriel.
- _priority. Spécifie la priorité du courriel.
- _to. Ajoute des destinataires au champ A du message.
- _cc. Ajoute des destinataires au champ Cc du message (envoyer une copie à).
- _bcc. Ajoute des destinataires au champ Cci du message (envoyer une copie invisible à).
- _subject. Spécifie le sujet du courriel.
- _encoding. Spécifie le codage du courriel.
- template. Permet d'ajouter une chaîne de texte à un message à partir de lignes de code JavaScript.
- _util. Objet utilitaire.
- _eventContextInformation. Contient des informations sur l'événement généré par la tâche actuelle, telles que le nom de l'événement et le statut d'approbation.
- _taskContextInformation. Contient un ensemble d'informations sur la tâche actuelle, telles que le nom de tâche, le nom de l'organisation et les événements constitutifs.

Ces objets sont décrits dans les sections suivantes.

_contentType

Spécifie le type de contenu du courriel.

Si aucun type de contenu n'est spécifié dans la variable _contentType, le type par défaut text/html sera appliqué.

Méthodes : aucune

Exemple :

```
<% _contentType = "text/html" ; %>
```

_priority

Spécifie la priorité du courriel. Indiquez 0 pour aucune priorité (valeur par défaut) et 1 pour une priorité élevé.

Méthodes : aucune

Exemple :

```
<% _priority = "1" ; %>
```

_to

Ajoute des destinataires au champ A du message.

La valeur de la variable _to est une chaîne JavaScript. Plusieurs destinataires peuvent être indiqués, mais la chaîne doit être conforme à la syntaxe JavaScript, tel qu'illustré dans l'exemple suivant.

Méthodes : aucune

Exemple :

```
<%
_to =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute") ;
_cc = "" ;
_bcc = "" ;
_subject = "Your new password ";
%>
```

Remarque : Lorsque les courriels alertent les participants que l'état d'une tâche est En attente et sous le contrôle du flux de travaux, l'objet _to est prérempli avec les adresses de ces participants. Vous ne pouvez pas utiliser l'objet _to dans un modèle En attente.

_cc

Ajoute des destinataires au champ Cc du message (envoyer une copie à).

La valeur de la variable _to est une chaîne JavaScript. Plusieurs destinataires peuvent être indiqués, mais la chaîne doit être conforme à la syntaxe JavaScript, tel qu'illustré dans l'exemple suivant.

Méthodes : aucune

Exemple :

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute") ;
%>
```

_bcc

Ajoute des destinataires au champ Cci du message (envoyer une copie invisible à).

Les adresses électroniques spécifiées dans ce champ n'apparaissent pas dans le courriel.

La valeur de la variable _to est une chaîne JavaScript. Plusieurs destinataires peuvent être indiqués, mais la chaîne doit être conforme à la syntaxe JavaScript, tel qu'illustré dans l'exemple suivant.

Méthodes : aucune

Exemple :

```
<%
_bcc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute") ;
%>
```

_subject

Spécifie le sujet du courriel.

Méthodes : aucune

Exemple :

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

_encoding

Spécifie le codage du courriel.

Si aucun codage n'est spécifié dans _encoding ou dans la variable LANG, il est possible que les caractères dans le courriel n'apparaissent pas correctement. Veillez à définir _encoding ou LANG pour les paramètres régionaux appropriés.

Méthodes : aucune

Exemple :

```
<% _encoding = "UTF-8"; %>
```

_additionalHeaders

_additionalHeaders

Spécifie des attributs d'en-tête de courriel supplémentaires dans le modèle de courriel.

Vous devez affecter une table de hachage() à cet attribut. Les noms et valeurs stockés dans la table de hachage doivent être des chaînes.

Exemple : Ajout d'attributs d'en-tête personnalisés

L'exemple suivant illustre l'ajout de deux attributs d'en-tête personnalisés : X-TCCCSWD et myheader :

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```

template

Permet d'ajouter une chaîne de texte à un message à partir de lignes de code JavaScript ; c'est-à-dire, les lignes dans la balise <% %>. La chaîne peut contenir des balises HTML, du texte statique, et/ou des valeurs variables renvoyées par des méthodes dans des objets CA Identity Manager implicites.

Remarque : L'objet de modèle n'est pas précédé du trait de soulignement (_).

Méthode :

- add(String)

  L'argument doit renvoyer une chaîne, y compris les appels aux méthodes dans un objet CA Identity Manager implicite. Dans l'exemple ci-après, consultez _eventContextInformation.getSecondaryObjectName().

Exemple :

```
<%
var secondaryType =        _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                              ObjectName()+" </b><br>");
   }
%>
```

_util

Objet utilitaire

Méthode :

- getNotifiers(String [,String])

  Renvoie des ID de courriel en fonction d'une règle de notification.

  Le premier argument prend en charge les règles de notification prédéfinies suivantes, placées entre guillemets :

  - "ADMIN". Envoie le courriel à l'administrateur qui a initialisé la tâche.
  - "USER". Envoie le courriel à l'utilisateur dans le contexte actuel.
  - "USER_MANAGER". Envoie le courriel au gestionnaire de l'utilisateur dans le contexte actuel.

Vous pouvez également référencer une règle de notification personnalisée créée avec l'API de règle de notification. Pour plus d'informations, reportez-vous au *manuel de programmation pour Java.*

Le deuxième argument est facultatif. Vous pouvez l'utiliser pour transmettre une ou plusieurs paires nom/valeur définies par l'utilisateur dans une règle de notification personnalisée. Séparez chaque paire nom/valeur par une virgule, au format suivant :

"*name1=value1,name2=value2*..."

Exemples :

```
<%

_to = _util.getNotifiers("ADMIN");_cc = "";
%>
<%
_to = _util.getNotifiers("MYRULE","type=loan,district=3");
_cc = "";
%>
```

Notification au gestionnaire d'un utilisateur

Vous pouvez utiliser la règle de notification USER_MANAGER pour envoyer un courriel au gestionnaire d'un utilisateur. CA Identity Manager utilise cette règle dans les modèles de courriel prenant en charge la certification des droits de l'utilisateur.

Remarque : La règle de notification USER_MANAGER s'applique uniquement aux événements ou aux tâches qui créent ou gèrent un utilisateur unique.

Etant donné le grand nombre de méthodes différentes permettant de spécifier une relation utilisateur-gestionnaire dans un répertoire d'utilisateurs, l'adaptateur de notification au gestionnaire d'utilisateurs par défaut résout cette relation en fonction d'une expression d'attribut spécifiée dans le deuxième paramètre de la méthode getNotifiers().

Exemple :

```
<%
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "";
%>
```

L'adaptateur de notification au gestionnaire d'utilisateurs prend en charge deux options de recherche :

- managerattribute **= <***Manager AttributeName***>**- où l'objet utilisateur conserve un attribut qui indique le nom unique ou l'ID d'utilisateur du gestionnaire de cet utilisateur.
- commonattribute **= <***AttributeName***>** - où l'utilisateur et son gestionnaire partagent une valeur d'attribut commune, telle que Service.

Configurez ces options de recherche dans les propriétés diverses d'un environnement dans la console de gestion CA Identity Manager.

Pour configurer la règle de notification USER_MANAGER :

1. Dans la console de gestion CA Identity Manager, sélectionnez Identity Manager Environments (Environnements CA Identity Manager). Puis, sélectionnez l'environnement pour lequel vous configurez la notification par courriel.
2. Sélectionnez Paramètres avancés (Advanced Settings), Miscellaneous Properties (Propriétés diverses).
3. Dans la page Miscellaneous Properties (Propriétés diverses), suivez la procédure de configuration pour l'option de recherche que vous voulez utiliser :
   - Pour utiliser l'option de recherche managerattribute=<Manager AttributeName> :
     a. Dans le champ Propriété, saisissez managerattribute.
     b. Dans le champ Valeur, saisissez l'attribut qui stocke le nom unique ou l'ID d'utilisateur du gestionnaire.
     c. Cliquez sur Ajouter.
     d. Cliquez sur Enregistrer.
   - Pour utiliser l'option de recherche commonattribute=<AttributeName> :
     a. Dans le champ Propriété, saisissez commonattribute.
     b. Dans le champ Valeur, saisissez l'attribut commun à l'utilisateur et à son gestionnaire.
     c. Cliquez sur Ajouter.
     d. Dans le champ Propriété, saisissez ismanagerfilter.

e. Dans le champ Valeur, saisissez une expression de recherche à l'aide de la syntaxe suivante :

<attribute> <operator> <filter>

Par exemple, le titre est égal à gestionnaire.

f. Cliquez sur Ajouter.

g. Cliquez sur Enregistrer.

Vous pouvez également écrire un adaptateur personnalisé et créer vos propres règles pour notifier le gestionnaire d'un utilisateur. Reportez-vous au *Manuel de programmation Java*.

_eventContextInformation

Contient des informations sur l'événement généré par la tâche actuelle, telles que le nom de l'événement et le statut d'approbation. Ces informations sont appelées informations de *contexte* de l'événement.

L'objet _eventContextInformation est créé à partir de la classe ExposedEventContextInformation dans le package com.netegrity.imapi.

Cet objet est disponible pour les courriels basés sur des modèles approuvés, en attente et rejetés. Pour plus d'informations sur ces modèles, consultez la section Modèles de courriel (page 534).

Méthodes : toutes les méthodes suivantes renvoient une chaîne.

Méthode	**Description**
getAdminName()	Renvoie le nom de l'utilisateur ayant soumis la tâche qui a généré l'événement. Désapprouvée dans CA IdentityMinder 5.6. Utilisez l'une des méthodes héritées suivantes : ■ getAdministrator() ■ getAdminFriendlyName()
getApprovalStatus()	Renvoie le statut d'approbation de l'événement. Une des valeurs suivantes : APPROVAL_STATUS_APPROVED APPROVAL_STATUS_REJECTED
getApprovalTime()	Renvoie l'heure d'approbation de l'événement.

Méthode	Description
getEventName()	Renvoie le nom de l'événement. Pour obtenir une liste de noms d'événement, consultez la section Evénements CA IdentityMinder.
getOrgName()	Renvoie le nom convivial de l'organisation dans laquelle la tâche est exécutée. Désapprouvée dans CA IdentityMinder 5.6. Utilisez la méthode héritée getObjectOrganizationFriendlyName().
getPassword()	Si les objets principaux sont de type USER, renvoie le mot de passe de l'utilisateur.
getPrimaryObjectTypeName()	Renvoie le type d'objet principal. Types d'objet principal renvoyés : ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getPrimaryObjectName()	Renvoie le nom de l'objet principal affecté par l'événement. Un *objet principal* est l'objet directement affecté par l'événement. Un *objet secondaire* est lié à l'objet principal, le cas échéant. Exemple : ■ Le type d'objet principal pour CreateUserEvent est USER. L'objet secondaire est celui dans lequel l'utilisateur est créé, c'est-à-dire ORGANIZATION. ■ Le type d'objet principal pour CreateAdminRoleEvent est ADMINROLE. Cet objet n'est pas lié à d'autres objets ; ainsi aucun objet secondaire n'existe. Avec un objet principal de type USER, getPrimaryObjectName() peut renvoyer John Jones.

Méthode	Description
getSecondaryObjectTypeName()	Si un objet secondaire a été affecté par l'événement, renvoie le type d'objet. Types d'objet secondaire renvoyés : ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getSecondaryObjectName()	Si un objet secondaire a été affecté par l'événement, renvoie le nom de l'objet. Pour obtenir des informations sur les objets principaux et secondaires, consultez getPrimaryObjectName(). Avec un objet secondaire de type ORGANIZATION, la méthode getSecondaryObjectName() peut renvoyer RH.

Remarque : Les méthodes en _eventContextInformation sont fournies via l'interface ExposedEventContextInformation. Etant donné que ExposedEventContextInformation hérite des méthodes de l'API CA IdentityMinder principale, _eventContextInformation peut également appeler ces méthodes à partir d'un modèle de courriel, avec les méthodes figurant dans le tableau ci-dessus. Pour plus d'informations sur ces méthodes héritées, consultez la section Méthodes supplémentaires (page 553).

Exemple : Notification par courriel sur un événement En attente :

```
<%

_cc = "" ;_bcc = "";
_subject = _eventContextInformation.getEventName() +
                                            " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:
<br><br><br>
Event: <b><%=_eventContextInformation.getEventName()%></b> <br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
</body>
</html>
```

Potentiel corps du courriel :

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**

Remarque : La valeur du champ De provient du fichier email.properties. Pour modifier la valeur, modifiez le fichier suivant :

<*iam_im.ear*>\config\com\netegrity\config\email.properties

où <*iam_im.ear*> est l'emplacement d'installation de CA IdentityMinder dans le domaine du serveur d'applications. Par exemple :

Pour WebLogic :

<*WebLogic_home*>\user_projects\<domain>\applications\iam_im.ear

Pour JBoss :

<*Identity Manager_home*>\jboss-3.2.2\server\default\deploy\iam_im.ear

Pour WebSphere :

<*rép_outils_admin_im*>\WebSphere-ear\iam_im.ear

Pour ajouter des informations supplémentaires sur l'utilisateur affecté par l'événement au courriel dans l'exemple précédent, ajoutez le texte similaire au suivant :

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>User information:</b><br>
Last Name: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
First Name: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
Full Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
Email: <b><%=user.getAttribute("%EMAIL%")%></b><br>
Organization Membership: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

Potentiel corps du courriel :

```
From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: CreateUserEvent
USER: Richard Ferrigamo
In ORGANIZATION: Mortgages & Loans
User information:
Last Name: Ferrigamo
First Name: Richard
Full Name: Richard Ferrigamo
Email: rferrigamo@mybank.org
Organization Membership: Mortgages & Loans
```

_taskContextInformation

Contient un ensemble d'informations sur la tâche actuelle, telles que le nom de tâche, le nom de l'organisation et les événements constitutifs. Ces informations sont appelées informations de *contexte* de la tâche.

Cet objet est disponible pour les courriels basés sur des modèles terminés. Pour plus d'informations sur ce modèle, consultez la section Modèles de courriel (page 534).

Méthodes : toutes les méthodes ci-après renvoient une chaîne, sauf la méthode getExposedEventContexts(), qui renvoie un vecteur Java.

Méthode	Description
getAdminName()	Renvoie le nom de l'utilisateur qui soumet la tâche. Désapprouvée dans CA Identity Manager 5.6. Utilisez l'une des méthodes héritées suivantes : ■ getAdministrator() ■ getAdminFriendlyName()
getExposedEventContexts()	Renvoie un vecteur Java de tous les événements associés à la tâche. Chaque objet dans le vecteur est un objet de contexte d'événement. Vous pouvez utiliser les méthodes répertoriées sous _eventContextInformation pour récupérer des informations de contexte d'un objet d'événement donné. L'objet renvoyé est un objet de vecteur Java standard. Vous pouvez utiliser l'une des méthodes de l'objet de vecteur (par exemple, get() et size()) pour gérer les éléments dans le vecteur.
getOrgName()	Renvoie le nom de l'organisation dans laquelle la tâche est exécutée. Désapprouvée dans CA Identity Manager 5.6. Utilisez la méthode héritée getObjectOrganizationFriendlyName().
getTaskName()	Renvoie le nom de la tâche en cours d'exécution. Désapprouvée dans CA Identity Manager 5.6. Utilisez l'une des méthodes héritées suivantes : ■ getAdminTask() ■ getTaskFriendlyName()

Remarque : Les méthodes sous _taskContextInformation sont fournies via l'interface ExposedTaskContextInformation. Etant donné que ExposedTaskContextInformation hérite des méthodes de l'API de CA Identity Manager principale, _taskContextInformation peut également appeler ces méthodes à partir d'un modèle de courriel, avec les méthodes figurant dans le tableau ci-dessus. Pour plus d'informations sur ces méthodes héritées, consultez la section Méthodes supplémentaires (page 553).

Exemple : Corps d'un modèle de notification par courriel pour la modification d'un mot de passe :

```
<%
var imsEventContexts
=              _taskContextInformation.getExposedEventContexts();
if(imsEventContexts != null)
   {
   for(var i=0;i<imsEventContexts.size();i++)
      {
      var eventContext = imsEventContexts.get(i);
      template.add("Hi "+
eventContext.getPrimaryObjectName()
           + ",");
      template.add("<br>Your new password is: <b>"+
                              eventContext.getPassword());</br>
      template.add("<hr>");
      }
   }
%>
```

Potentiel corps du courriel :

Hi Victor Imperioso,
Your new password is: LFH7F1226

Méthodes supplémentaires

Les méthodes sous _taskContextInformation et _eventContextInformation sont fournies via les objets ExposedTaskContextInformation et ExposedEventContextInformation de CA Identity Manager, respectivement.

Ces objets héritent des méthodes dans l'API CA Identity Manager principale. Par conséquent, les méthodes héritées sont également disponibles dans _taskContextInformation et _eventContextInformation.

Les méthodes suivantes héritées de l'objet TaskInfo sont notamment utiles pour un modèle de courriel :

- getAdministrator(). Récupère un objet d'utilisateur pour l'administrateur qui exécute la tâche actuelle.
- getAdminTask(). Récupère un objet AdminTask pour la tâche actuelle.

Ces objets récupérés permettent d'insérer des informations spécifiques à l'administrateur et à la tâche dans un courriel. Exemple :

```
<!-- Define the E-mail Properties --->

<%
   _cc = "" ;
   _bcc = "" ;
   _subject = _eventContextInformation.getEventName() +
                                              " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:<br>
<br>
User <b><%= _eventContextInformation.getAdministrator().
               getAttribute(Packages.com.netegrity.llsdk6.imsapi.
                managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
               from department <b><%= _eventContextInformation.
               getAdministrator().getOrg(null).getFriendlyName()
               %></b> initiated task <b><%= _eventContextInformation.
               getAdminTask().getFriendlyName() %></b>at
<b><%=                _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
<font color="green">Details: </font><b><%=_eventContextInformation.
                                          getEventName()%></b><br>
<font color="green"><%=_eventContextInformation.
                              getPrimaryObjectTypeName()%>:</font>
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>
                                                      was modified
<br>
<font color="green">Updated Attributes:</font>
<table border="1">
<tr>
  [assign the value for TD in your book]<b>Name</b></td>
  [assign the value for TD in your book]<b>Value</b></td>
</tr>
```

```
<%
   var event = _eventContextInformation.getEvent();
   if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
      var user = event.getUser();
      var attributes = user.getAttributes().keys();
      while(attributes.hasMoreElements()) {
         var attr = attributes.nextElement();
         var value = user.getAttribute(attr);
         if(user.hasAttributeChanged(attr)) {
            template.add("<tr>[assign the value for TD in your book]" + attr
+"</td>");
            template.add("[assign the value for TD in your book]" + value
+"</td></tr>");
         }
      }
   }
%>
</table>
<br>
</body>
</html>
```

Potentiel corps du courriel :

The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**
User: **John Jones** was modified
Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

Pour plus d'informations sur les méthodes héritées disponibles pour l'API de modèle de courriel, consultez les objets ExposedTaskContextInformation et ExposedEventContextInformation dans l'outil Javadoc de CA Identity Manager.

Flux de sortie standard Java

Un courriel peut également effectuer des appels au flux de sortie standard Java à partir de la balise JavaScript (<% %>). Par exemple, l'appel suivant envoie le message Terminé à la console du serveur :

```
<%
...       // JavaScript processing
out.println("Done.");
%>
```

Référence de l'outil Javadoc

Pour plus d'informations sur les objets ExposedTaskContextInformation et ExposedEventContextInformation, notamment les méthodes qu'ils héritent de l'API CA Identity Manager principale, consultez le document Javadoc de CA Identity Manager.

Les pages du document de l'outil Javadoc sont intégrées à une version HTML du manuel de programmation pour Java, disponible dans la bibliothèque CA Identity Manager.

Déploiement de modèle de courriel

Lorsque CA IdentityMinder est sur le point d'envoyer un courriel, il recherche des modèles à partir desquels générer le courriel dans l'emplacement racine suivant dans votre serveur d'applications :

iam_im.ear\custom\emailTemplates

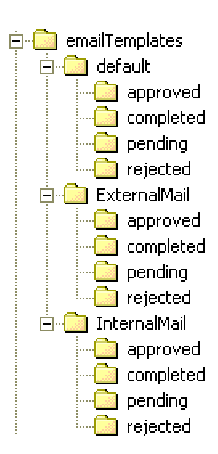
Les modèles de courriel déployés dans cet emplacement racine sont contenus dans des ensembles de modèle qui ont la même structure de répertoires ; c'est-à-dire que chaque ensemble contient un répertoire approuvé, un répertoire terminé, un répertoire en attente et un répertoire rejeté.

Ensembles de modèles

Vous pouvez déployer plusieurs ensembles de modèles de courriel sous emailTemplates. Par exemple, lors de l'installation, l'ensemble suivant de modèles de courriel est créé sous iam_im.ear\custom\emailTemplates :

```
default\approved
default\completed
default\pending
default\rejected
```

L'ensemble de modèles de courriel par défaut contient les modèles installés décrits à la section Modèles de courriel (page 534). Vous pouvez ajouter des modèles personnalisés dans l'ensemble par défaut. Vous pouvez également déployer d'autres ensembles de modèles de courriel dans des structures de répertoires que vous définissez au même niveau que l'ensemble par défaut. Par exemple, iam_im.ear\custom peut contenir les modèles de courriel déployés suivants :



Remarque : Pour plus d'informations sur la sélection par CA IdentityMinder d'un modèle de courriel particulier dans un ensemble de modèles, consultez la section Répertoires de modèles (page 536).

Spécification d'un ensemble de modèles pour un environnement

Lors de la configuration d'un courriel pour un environnement CA Identity Manager, spécifiez l'ensemble de modèles de courriel que vous voulez utiliser pour cet environnement. Pour plus d'informations sur la configuration de courriel pour un environnement CA Identity Manager, consultez le *Manuel de configuration de CA Identity Manager*.

Noms de modèle

Les répertoires dans un ensemble de modèles personnalisés doivent contenir des modèles par défaut portant le même nom que ceux installés dans l'ensemble de modèles par défaut. Les noms par défaut sont répertoriés sous Modèles de courriel (page 534). CA Identity Manager utilise les modèles par défaut lorsqu'il ne trouve aucun autre modèle portant un nom correspondant à la tâche ou à l'événement en cours d'exécution.

Vous pouvez également ajouter des modèles supplémentaires à un ou plusieurs répertoires dans un ensemble de modèles si vous voulez qu'un courriel soit généré à partir d'un modèle particulier. Procédez comme suit :

- Affectez au modèle le même nom que la tâche ou l'événement pour lequel le courriel sera généré.
- Placez le modèle dans le répertoire associé à l'état de la tâche ou de l'événement pour lequel le courriel sera généré.

Par exemple, si vous voulez que les courriels soient générés à partir d'un modèle particulier lorsqu'un événement CreateUserEvent est rejeté, placez un modèle nommé CreateUserEvent.tmpl dans le répertoire rejeté de l'ensemble de modèles de l'environnement.

Chapitre 20: Persistance des tâches

Ce chapitre traite des sujets suivants :

Archivage et nettoyage de la mémoire automatisés dans la base de données de persistance des tâches

Dans cette version, les administrateurs peuvent planifier et modifier des jobs à l'aide de paramètres spécifiques et de la tâche Nettoyer les tâches soumises, afin de nettoyer et d'archiver les informations relatives aux événements et aux tâches dans la base de données de persistance des tâches ; ils peuvent également supprimer les tâches récurrentes, si nécessaire.

Pour lancer l'assistant, accédez à l'onglet Système, puis sélectionnez Nettoyer les tâches soumises. L'assistant vous guidera tout au long du processus de configuration et de planification des jobs et vous aidera à déterminer si certaines données doivent être archivées. Pour supprimer les jobs récurrents, accédez à l'onglet Système, puis sélectionnez Supprimer les tâches récurrentes.

La planification du nettoyage des tâches et de l'archivage des données de tâches permet de réduire considérablement les problèmes de performance ou d'interruptions du système. Grâce à la fonctionnalité d'archivage, vous pouvez sauvegarder les tâches dans la base de données d'archivage avant de les supprimer de la base de données d'exécution. Pour revenir à l'étape précédente et afficher la liste des tâches supprimées et archivées, sélectionnez Rechercher les archives des tâches soumises.

Onglet Répétition

Utilisez cet onglet pour planifier votre job. Cet onglet dispose des champs suivants.

Exécuter

Permet d'exécuter le job immédiatement.

Planifier un nouveau job

Permet de planifier un nouveau job.

Modifier le job actuel

Spécifie que vous voulez modifier un job existant.

Remarque : Ce champ apparaît uniquement si un job a déjà été planifié pour cette tâche.

Nom du job

Spécifie le nom du job que vous souhaitez créer ou modifier.

Fuseau horaire

Spécifie le fuseau horaire du serveur.

Remarque : Si votre fuseau horaire est différent de celui du serveur, une zone déroulante permet de sélectionner votre fuseau horaire ou celui du serveur lorsque vous planifiez un nouveau job. Vous ne pouvez pas modifier le fuseau horaire lorsque vous modifiez un job existant.

Planification hebdomadaire

Spécifie que le job est exécuté un ou plusieurs jours ou une heure spécifiques de la semaine.

Planification avancée

Spécifie les informations de planification supplémentaires.

Jour de la semaine

Spécifie le ou les jours de la semaine pendant lesquels le job est exécuté.

Heure d'exécution

Spécifie l'heure, au format 24 heures, à laquelle le job est exécuté. Par exemple, 14 h 15.

Expression Cron

Pour obtenir des informations sur le remplissage de ce champ, reportez-vous à l'adresse suivante :

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Remarque : Ce champ apparaît lorsque la planification avancée est sélectionnée.

Informations complémentaires

Exécution immédiate d'un job (page 562)
Planification d'un nouveau job (page 562)
Modification d'un job existant (page 563)
Suppression d'une tâche récurrente (page 563)

Onglet Nettoyer les tâches soumises

Cet onglet permet de spécifier l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de la tâche. Lorsque tous les champs obligatoires sont remplis, cliquez sur Terminer. Cet onglet dispose des champs suivants.

Age minimal

Spécifie l'âge minimum des tâches dont l'état final (Terminé, Echec, Rejet, Annulation ou Abandon) doit être nettoyé. Par exemple, si 1 mois est spécifié, toutes les tâches ayant atteint un état final au cours du dernier mois sont conservées. Toutes les tâches ayant atteint un état final il y a plusieurs mois font l'objet d'un nettoyage et d'un archivage.

Ce champ est obligatoire.

Archiver

Sauvegarde les tâches dans l'archivage de la base de données avant suppression de la base de données d'exécution.

Une fois la tâche exécutée, si l'archive est sélectionnée, les données sont soumises à la base de données d'archivage et supprimées de la base de données de persistance des tâches d'exécution. Les données ne sont supprimées qu'une fois correctement soumises à la base de données d'archivage.

Délai d'expiration de l'audit

Spécifie le délai avant nettoyage des tâches présentant l'état Audit. Les tâches présentant l'état Audit n'atteignent pas l'état final tant que ce délai n'est pas écoulé. Les tâches présentant l'état Audit n'ont été soumises

Limite de temps

Limite le nettoyage à une durée spécifique.

Limite de la tâche

Limite le nettoyage à une nombre de tâches spécifique.

Exécution immédiate d'un job

Pour exécuter un job immédiatement, utilisez l'assistant Nettoyer les tâches soumises.

Dans l'onglet Système :

1. Sélectionnez Nettoyer les tâches soumises dans le volet gauche.

   La fenêtre Répétition de l'assistant s'ouvre.

2. Sélectionnez Exécuter, puis Suivant.

   La fenêtre Nettoyer les tâches soumises de l'assistant s'ouvre.

3. Entrez les informations relatives à l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de tâche, puis cliquez sur Terminer.

   Le job est soumis immédiatement.

Planification d'un nouveau job

Pour planifier un nouveau job, utilisez l'assistant Nettoyer les tâches soumises.

Dans l'onglet Système :

1. Sélectionnez Nettoyer les tâches soumises dans le volet gauche.

   La fenêtre Répétition s'ouvre.

2. Sélectionnez Planifier un nouveau job, entrez le nom et les informations de planification du job, puis cliquez sur Suivant.

   La fenêtre Nettoyer les tâches soumises s'ouvre.

3. Entrez les informations relatives à l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de tâche, puis cliquez sur Terminer.

   Le nouveau job est planifié.

Modification d'un job existant

Pour modifier un job existant, utilisez l'assistant Nettoyer les tâches soumises.

Dans l'onglet Système :

1. Sélectionnez Nettoyer les tâches soumises dans le volet gauche.

   La fenêtre Répétition s'ouvre.

2. Sélectionnez Modifier le job actuel et choisissez un job existant, modifiez les informations de planification, puis cliquez sur Suivant.

   La fenêtre Nettoyer les tâches soumises s'ouvre.

3. Modifiez les informations relatives à l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de tâche, puis cliquez sur Terminer.

   Le job existant est modifié.

Suppression d'une tâche récurrente

Pour supprimer une tâche récurrente, procédez comme suit :

Dans Afficher les tâches soumises

1. Sélectionnez Supprimer une tâche récurrente.
2. Sélectionnez la tâche que vous souhaitez supprimer.
3. Cliquez sur Soumettre.

Migration de la base de données de persistance des tâches

Dans les versions précédentes, la migration était effectuée à la hâte et à l'aide de la console de gestion. Un outil de migration de ligne de commande est fourni pour supprimer des goulots d'étranglement de performances lors de la migration de quantité importante de tâches. Vous pouvez également affiner le réglage de la migration vers un environnement spécifique, l'état des tâches et les tâches créées et exécutées pendant une plage de dates spécifique. L'outil de ligne de commande, runmigration, se trouve dans le dossier suivant :

```
admin_tools/tools/tpmigration
```

Pour migrer la base de données de persistance des tâches, vous devez procéder comme suit :

1. Mettez à jour le fichier tpmigration125.properties.
2. Définissez la variable JAVA_HOME.
3. Exécutez l'outil runmigration.

Mettez à jour le fichier tpmigration125.properties.

Pour configurer la migration de base de données de persistance des tâches, vous devez mettre à jour le fichier tpmigration.properties avec le référentiel d'objets et les informations de persistance des tâches comprenant les valeurs du référentiel. Le fichier tpmigration125.properties se trouve à l'emplacement suivant :

<IAM suite folder>/tools/tpmigration/com/ca/tp/migratetpto125

Pour configurer la migration, renseignez les informations suivantes dans le fichier de propriétés :

```
############################################################
# Le référentiel d'objets est requis pour obtenir les détails de l'environnement.
############################################################
os.db.hostname=<nom d'hôte>
os.db.dbname=<nom base de données ou SID>
os.db.username=<nom d'utilisateur BdD>
os.db.password=<mot de passe d'utilisateur BdD>
os.db.port=<numéro de port BdD>
os.db.dbType=<type de base de données.  Par ex. pour SQL server sql2005 et pour Oracle
'oracle'>

############################################################
# Données de persistance des tâches où se trouvent les tables anciennes et nouvelles.
############################################################
tp.db.hostname=<nom d'hôte>
tp.db.dbname=<nom base de données ou SID>tp
tp.db.username=<nom d'utilisateur BdD>
tp.db.password=<mot de passe d'utilisateur BdD>
tp.db.port=<numéro de port BdD>
tp.db.dbType=<type de base de données.  Par ex. pour SQL server sql2005 et pour Oracle
'oracle'>
```

Définition de la variable JAVA_HOME.

Pour le fonctionnement correct de l'outil runmigration, veillez à définir la variable d'environnement JAVA_HOME.

Exécution de l'outil runmigration

Pour démarrer la migration, suivez la procédure suivante :

Dans une ligne de commande :

1. Exécutez l'outil runmigration.

   Sous Windows :

   `runmigration.bat`

   Sous UNIX :

   `runmigration.sh`

2. Entrez les informations suivantes :

   - Alias de protection de l'environnement (Tout pour tous les environnements)

     Remarque : Si vous ne spécifiez pas Tout, vous pouvez entrer un seul environnement.

   - Etat de la tâche
     Remarque : Si vous ne spécifiez pas Tout, vous pouvez entrer un seul état de tâche.

   - La version CA IdentityMinder à partir de laquelle effectuer la migration (1-8.x, 2-12.0)

   - Indiquez si vous souhaitez spécifier une plage de dates pour les tâches à migrer (o/n).

     Remarque : Si vous choisissez o, vous devez saisir les éléments suivants :

     - Saisissez la date de début (mm/jj/aa)
     - Saisissez la date de fin (mm/jj/aa)

   La migration démarre.

A l'issue de la migration, le statut indique le nombre de tâches migrées.

Chapitre 21: Rôles d'accès

Les rôles d'accès permettent de fournir des droits dans CA IdentityMinder ou une autre application. Par exemple, vous pouvez utiliser les rôles d'accès pour effectuer les tâches suivantes :

- Fournir l'accès indirect à un attribut d'utilisateur
- Créer des expressions complexes
- Définir un attribut dans un profil d'utilisateur, qui est utilisé par une autre application pour définir des droits

Les rôles d'accès sont similaires aux stratégies d'identité, car ils appliquent un ensemble de modifications à un utilisateur ou à un groupe d'utilisateurs. Toutefois, lorsque vous utilisez un rôle d'accès pour appliquer des modifications, vous pouvez voir les utilisateurs auxquels les modifications s'appliquent en affichant les membres du rôle d'accès.

Dans la plupart des cas, les rôles d'accès ne sont pas associés à des tâches.

Remarque : Lorsque CA IdentityMinder s'intègre à CA SiteMinder, les rôles d'accès peuvent également fournir l'accès aux applications qui sont protégées par CA SiteMinder. Dans ce cas, les rôles d'accès incluent des tâches d'accès. Pour plus d'informations, reportez-vous au chapitre relatif à l'intégration de SiteMinder dans le manuel *Configuration Guide*.

Ce chapitre traite des sujets suivants :

Procédure de gestion des droits à l'aide des rôles d'accès

Vous pouvez utiliser les rôles d'accès pour gérer les droits en spécifiant les actions de modification qui se produisent lorsqu'un utilisateur est ajouté ou supprimé comme membre ou administrateur d'un rôle.

Pour utiliser des rôles d'accès, procédez comme suit :

1. Un administrateur crée un rôle d'accès.
2. Dans l'onglet Membres, l'administrateur spécifie des actions d'ajout ou de suppression qui déterminent les actions entreprises par CA IdentityMinder lorsque le rôle d'accès est affecté à un utilisateur.
3. L'administrateur spécifie les stratégies d'administrateur et de propriétaire, si nécessaire, et soumet la tâche pour créer le rôle d'accès.
4. Les administrateurs de rôles d'accès affectent le rôle d'accès aux utilisateurs.
5. CA IdentityMinder effectue les actions d'ajout spécifiées dans le rôle.

Exemple : Modification indirecte d'attributs de profil

Vous pouvez utiliser les rôles d'accès pour changer indirectement un attribut dans le profil d'un utilisateur. Par exemple, une société peut empêcher les utilisateurs de modifier directement le titre d'un autre utilisateur. Cette société peut créer un rôle d'accès qui permet de changer un titre. L'administrateur peut alors affecter ce rôle à un utilisateur.

Pour changer indirectement un attribut, définissez les actions de modification pour le rôle d'accès. Lorsqu'un administrateur affecte le rôle, l'action de modification peut appliquer une ou plusieurs modifications à un attribut dans le profil de l'utilisateur.

Pour utiliser un rôle d'accès pour modifier indirectement un attribut, procédez comme suit :

1. Créez un rôle d'accès.
2. Dans l'onglet Membres, activez la case à cocher suivante : Les administrateurs peuvent ajouter des membres à ce rôle et les en supprimer. Cliquez ensuite sur l'icône de la flèche.

   CA IdentityMinder affiche des champs Action Ajouter et Action Supprimer supplémentaires.
3. Dans les champs Action Ajouter et Action Supprimer, sélectionnez une action dans la zone de liste.

   CA IdentityMinder affiche des champs supplémentaires selon l'option que vous avez sélectionnée.

4. Configurez les actions Ajouter ou Supprimer si nécessaire.
5. Sélectionnez l'onglet Administrateur pour spécifier les administrateurs qui peuvent ajouter des membres au rôle d'accès créé.
6. Sélectionnez l'onglet Propriétaires pour spécifier les administrateurs qui peuvent modifier la définition du rôle d'accès.
7. Cliquez sur Soumettre pour terminer la création du rôle d'accès.
8. Affectez le rôle d'accès à des utilisateurs, si nécessaire.

Créez un rôle d'accès.

La création d'un rôle d'accès se déroule en plusieurs étapes..

Début de la création d'un rôle d'accès

1. Connectez-vous à un compte Identity Manager avec un rôle incluant une tâche de création de rôle d'accès.
2. Cliquez sur Rôles d'accès, puis sur Créer un rôle d'accès.

   Choisissez l'option de création de rôle ou de copie d'un rôle. Si vous sélectionnez Copier, recherchez le rôle.
3. Passez à la section suivante, Définition du profil d'un rôle d'accès.

Définition du profil d'un rôle d'accès

Définition du profil d'un rôle d'accès

1. Entrez un nom et une description, puis spécifiez les attributs personnalisés définis pour le rôle.

   Remarque : Dans l'onglet Profil, vous pouvez spécifier des attributs personnalisés qui indiquent des informations supplémentaires sur les rôles d'accès. Vous pouvez utiliser ces dernières pour faciliter les recherches de rôles dans les environnements comprenant un nombre important de rôles.

2. Sélectionnez Activé si le rôle peut être mis à la disposition des utilisateurs dès qu'il est créé.

3. Passez à la section suivante, Définition de stratégies de membres pour un rôle d'accès (page 570).

Informations complémentaires :

Attributs personnalisés définis par l'utilisateur pour les rôles (page 53)

Définition de stratégies de membres pour un rôle d'accès

Dans l'onglet Membres, procédez comme suit.

1. Sélectionnez Ajouter pour définir les stratégies de membres.

2. (Facultatif) Dans la page Stratégie de membre, définissez une règle de membre déterminant qui doit pouvoir utiliser ce rôle.

   Ceci affecte automatiquement le rôle aux utilisateurs correspondant aux critères de la stratégie de membre.

3. Vérifiez que la stratégie de membre s'affiche dans l'onglet Membres.

   Pour modifier une stratégie, cliquez sur la flèche située à gauche. Pour la supprimer, cliquez sur l'icône représentant un signe moins.

4. Dans l'onglet Membres, cochez la case Les administrateurs peuvent ajouter et supprimer des membres à ce rôle.

   Une fois cette fonctionnalité activée, définissez l'action d'ajout et l'action de suppression. Ces actions définissent ce qui se produit lorsqu'un utilisateur est ajouté ou supprimé en tant que membre du rôle.

5. Passez à la section suivante, Définition de stratégies d'administration pour un rôle d'accès (page 571).

Définition de stratégies de membres pour un rôle d'accès

Dans l'onglet Administrateurs :

1. Si vous souhaitez que l'option Gérer les administrateurs soit disponible, cochez la case Les administrateurs peuvent ajouter des administrateurs à ce rôle et les en supprimer.

   Une fois cette fonctionnalité activée, définissez les actions devant se produire lorsqu'un utilisateur est ajouté ou supprimé en tant qu'administrateur du rôle.

2. Dans l'onglet Administrateurs, ajoutez des stratégies d'administration incluant des règles d'administration et de portée et des droits d'administrateur. Chaque stratégie nécessite au moins un droit (Gérer les membres ou Gérer les administrateurs).

   Vous pouvez ajouter plusieurs stratégies d'administration comportant différentes règles et différents droits pour les administrateurs qui observent la règle.

3. Pour modifier une stratégie, cliquez sur la flèche située à gauche. Pour la supprimer, cliquez sur l'icône représentant un signe moins.

4. Passez à la section suivante, Définition de stratégies de membres pour un rôle d'accès (page 571).

Définition de règles de propriété pour un rôle d'accès

Dans l'onglet Propriétaires :

1. Définissez des règles de propriété, qui déterminent quels utilisateurs peuvent modifier le rôle.

2. Cliquez sur Soumettre.

   Un message s'affiche indiquant que la tâche a été soumise. Il peut se produire un retard temporaire avant qu'un utilisateur puisse utiliser le rôle.

Chapitre 22: Tâches système

Ce chapitre traite des sujets suivants :

Tâches système par défaut

CA IdentityMinder inclut les tâches suivantes, qui aident les administrateurs à gérer un environnement CA IdentityMinder :

- Tâche Afficher les tâches soumises

  permet aux administrateurs d'afficher l'état des tâches dans l'environnement. supprime également les tâches obsolètes des fenêtres d'affichage des tâches soumises.

- Tâches du chargeur en bloc

  Charge des fichiers d'insertion qui servent à manipuler de grands nombres d'objets gérés simultanément.

- Tâches en bloc

  Permet d'exécuter une tâche sur un objet, tel qu'un utilisateur, sur la base des attributs de ce dernier, comme le service, la ville, la date de résiliation, etc. Vous pouvez exécuter cette tâche périodiquement ; par exemple, tous les samedis.

  Vous pouvez également utiliser cette tâche pour apporter des modifications d'utilisateurs en bloc.

- Tâches Sélectionner des données de boîte

  permet aux administrateurs de télécharger des fichiers utilisés pour remplir les options dans les champs, comme sélectionner des boîtes dans les tâches d'administration.

- Tâches Gestionnaire d'attributs logiques

  permet aux administrateurs de gérer des attributs logiques, qui servent à afficher des attributs de magasins d'utilisateurs (appelés attributs physiques) dans un format convivial sur des fenêtres de tâches.

- Tâches de gestion des connexions JDBC

  Configure les détails de connexion du serveur de base de données dans CA IdentityMinder.

- Tâches de courriel

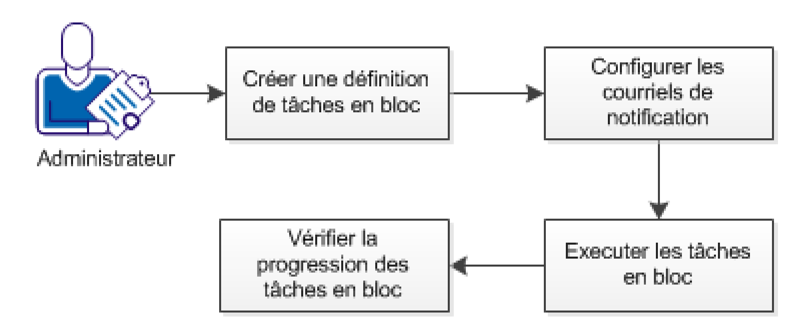
  Permet de gérer les stratégies de notification par courriel.

Procédure de modification en bloc des objets filtrés

Les tâches en bloc permettent d'effectuer les actions suivantes :

- Exécuter une tâche sur un objet, tel qu'un utilisateur, sur la base des attributs de ce dernier, comme le service, la ville, la date de résiliation, etc.
- Exécuter périodiquement une tâche sur des objets spécifiques (tous les samedis, par exemple).
- Effectuer des modifications d'utilisateurs en bloc, comme apporter des changements à tous les utilisateurs d'un service spécifique.

Cette fonction est différente de la fonction de tâche planifiée, car elle propose un filtre d'ensemble. En effet, contrairement aux tâches planifiées, l'ensemble d'objets affectés par une tâche en bloc n'est pas connu au moment où vous configurez cette dernière. De plus, les tâches en bloc concernent de nombreux objets, alors que celles planifiées n'en affectent qu'un seul.



Procédez comme suit:

1. Créez une définition de tâches en bloc (page 575).
2. (Facultatif) Configurez les courriels de notification pour des tâches en bloc (page 580).
3. Exécutez les tâches en bloc (page 580).
4. Vérifiez la progression des tâches en bloc (page 582).

Création d'une définition de tâches en bloc

Pour exécuter une tâche en bloc, commencez par créer une définition de tâches en bloc. Dans la console d'utilisateur, accédez à Système, Tâches en bloc, Créer une définition de tâches en bloc. Ses différents composants sont les suivants :

- L'auteur de la tâche
- Le type d'objet
- La tâche à effectuer
- Le filtre d'ensemble

Configuration de l'onglet Profil des tâches en bloc

L'onglet Profil permet de définir l'auteur des tâches en bloc, les tâches effectuées et le type d'objet sur lequel les exécuter. Les champs suivants doivent être configurés.

Nom

Définit le nom de l'ensemble de tâches.

Description

Explique le cas d'utilisation des tâches en bloc.

Auteur

Définit l'utilisateur qui exécute les tâches en bloc une fois déclenchées. Par défaut, l'auteur correspond à l'utilisateur qui définit les tâches en bloc.

La portée d'utilisateur par défaut du rôle Gestionnaire de tâches en bloc permet uniquement à un utilisateur de se définir lui-même comme auteur. Cette restriction évite des problèmes de sécurité, tels qu'un utilisateur qui dissimulerait son identité en désignant un autre utilisateur comme auteur lors de l'exécution de tâches en bloc.

Toutefois, vous pouvez utiliser ce champ pour effectuer des tâches en bloc pour un autre utilisateur (par exemple, un administrateur système qui exécuterait des tâches en bloc sur des utilisateurs pour le compte du directeur des Ressources humaines). Pour autoriser des utilisateurs de tâches en bloc à définir le nom de l'auteur sur celui d'un autre utilisateur, modifiez la portée d'utilisateur du rôle Gestionnaire de tâches en bloc.

Remarque : L'utilisateur que vous choisissez comme auteur affecte les tâches disponibles et les résultats de filtre d'ensemble puisqu'ils dépendent de la portée de l'auteur.

Type d'objet

Définit le type d'objet modifié par une tâche en bloc. Vous pouvez ajouter des types d'objet à la liste déroulante en modifiant le champ Types d'objet dans la configuration de l'onglet Profil. Pour modifier la configuration de l'onglet Profil, modifiez la tâche d'administration qui inclut la liste déroulante, sélectionnez l'onglet Onglets et modifiez l'onglet Profil.

Par défaut : types d'objet Utilisateur uniquement.

Remarque :

- Si vous ajoutez des types d'objet, modifiez l'onglet Profil des deux tâches : Créer *et* Modifier.
- Si vous ajoutez des types d'objet, assurez-vous d'ajouter des règles de portée pour ce type d'objet sur le rôle.

Tâche

Spécifie la tâche à effectuer sur les objets qui satisfont aux critères du filtre d'ensemble. Cette liste de tâches inclut la plupart des tâches d'administration, excepté les tâches suivantes.

- Tâches de type Afficher ou Créer (par exemple : Afficher l'utilisateur ou Créer un utilisateur)
- Tâches d'approbation

Remarque : Toutes les tâches ne sont pas accessibles à tous les utilisateurs. La liste des tâches dépend en effet du type d'objet et de la portée de l'auteur.

(Facultatif) Attributs

Définissez une liste d'attributs (page 577) à définir pour les objets qui correspondent aux critères du filtre d'ensemble. Ces attributs sont utiles pour les tâches qui impliquent des modifications d'attributs, telles que Modifier un utilisateur. Par exemple, vous pouvez sélectionner Nom du service comme attribut et Ventes comme valeur, de sorte que pour chaque utilisateur correspondant au filtre d'ensemble, le système change l'attribut Nom du service en Ventes.

Définition d'attributs facultatifs

Vous pouvez ajouter des attributs facultatifs si vous souhaitez modifier les attributs des objets renvoyés par le filtre d'ensemble.

Pour définir des attributs facultatifs

1. Cliquez sur le bouton Attributs.

   Une liste déroulante des attributs associés à la tâche s'affiche.

2. Sélectionnez l'attribut à définir.
3. Cliquez sur Ajouter (bouton plus).

   Une nouvelle ligne s'affiche dans un tableau avec une zone de texte Valeurs vide en regard de l'attribut.

4. Entrez les valeurs à définir pour l'attribut.
5. Répétez les étapes 2 à 4 pour chacun des attributs à définir.
6. Cliquez sur Ok.

Remarque : Lorsque vous sélectionnez un attribut à valeurs multiples, vous pouvez cliquer sur le bouton Ajouter (plus) pour définir plusieurs valeurs.

Onglet Ensemble de tâches en bloc

L'onglet Ensemble permet de rechercher les objets auxquels les tâches en bloc s'appliquent. Vous pouvez définir le filtre d'ensemble à l'aide des champs suivants.

Filtre d'objets

Définit l'ensemble d'objets à l'aide de filtres standard. Les attributs disponibles pour la recherche dépendent du type d'objet sélectionné sous l'onglet Profil des tâches en bloc.

Filtre de dates

Affine le filtre d'ensemble sur la base d'attributs contenant des dates (page 578), tels qu'un attribut de date d'embauche.

Format de date

Définit le format de date utilisé par le filtre de dates.

Aperçu

Affiche la liste des objets correspondant aux critères du filtre d'ensemble lorsque vous cliquez sur le bouton Aperçu. Ce bouton permet de vérifier que le filtre est bien configuré, mais le résultat du filtre peut changer au fil du temps. Dès lors, cette liste ne doit *pas* être utilisée pour désigner des objets qui seront modifiés ultérieurement.

Remarque : Les filtres de système privilégient l'opérateur OU plutôt que l'opérateur ET. Par exemple, le filtre "Ville Egal à Paris **ET** Service Egal à Ventes **OU** Service Egal à Achats" est traité comme "(Ville Egal à Paris) **ET** (Service Egal à Ventes **OU** Service Egal à Achats)".

Composants du filtre de dates

L'application de filtres de dates dans les tâches en bloc est utile dans la mesure où les ensembles affectés peuvent changer chaque jour. Par exemple, un filtre d'objets qui recherche les utilisateurs dont la date d'expiration est passée peut changer tous les jours.

Important : Si les objets sont dans un référentiel d'utilisateurs LDAP, les recherches de dates peuvent considérablement réduire les performances étant donné que les dates sont représentées sous forme de chaînes régulières.

Le filtre de dates comporte les champs suivants :

Attribut

Définit un attribut de l'objet qui contient une date. Tous les attributs de l'objet sont disponibles. Si le filtre utilise un attribut, le système suppose que ce dernier comporte une date.

Les valeurs des attributs doivent respecter le format de date défini sous l'onglet Ensemble. Les objets dont le format de date n'est pas valide sont ignorés.

Opérateur

Fait référence à des dates antérieures ou postérieures à la date du jour.

Décalage en jours

Définit un intervalle de temps par rapport à la date du jour. Par exemple, si vous souhaitez envoyer un courriel à tous les utilisateurs dont le profil expire dans la semaine à venir, vous devez utiliser l'opérateur "Au plus tard aujourd'hui" et la valeur 7 pour le décalage, ce qui signifie 7 jours à partir de la date actuelle. En revanche, si vous définissez le décalage sur -7, le courriel sera envoyé à tous les utilisateurs pour qui la date d'expiration remonte à plus d'une semaine. Le tableau ci-dessous récapitule le comportement du champ Décalage en jours :

Date du jour	Opérateur	Décalage en jours	Résultat
1/10/2010	Au plus tard aujourd'hui	7	Date égale ou antérieure au 17/01/10
1/10/2010	Au plus tard aujourd'hui	-7	Date égale ou antérieure au 03/01/2010
1/10/2010	Au plus tôt aujourd'hui	7	Date égale ou postérieure au 17/01/10
1/10/2010	Au plus tôt aujourd'hui	-7	Date égale ou postérieure au 03/01/2010

Configuration des courriels de notification pour des tâches en bloc

Dans certains environnements, les courriels de notification des opérations en bloc sont configurés par défaut. Pour vérifier si les courriels de notification des opérations en bloc sont configurées dans votre système, cliquez sur Système, Courriel, Afficher un courriel et recherchez le terme bloc.

Si aucune notification par courriel n'est configurée dans votre environnement, configurez le courriel qui est envoyé à l'issue d'une opération en bloc.

Procédez comme suit:

1. Dans la console d'utilisateur, cliquez sur Système, Courriel, Créer un courriel.
2. Dans l'onglet Profil, renseignez les champs requis.
3. Dans l'onglet Planification de l'envoi, effectuez les étapes suivantes :
   a. Sélectionnez Fin de la tâche dans le premier champ.
   b. Sélectionnez Exécuter les tâches en bloc dans le deuxième champ.
4. Remplissez les onglets Destinataires et Contenu, puis cliquez sur Soumettre.

   Les notifications par courriel sont configurées pour les tâches en bloc.

Exécuter les tâches en bloc

La tâche Exécuter les tâches en bloc permet de planifier des tâches en bloc ou de les démarrer manuellement tout de suite. Les tâches en bloc sont généralement planifiées, mais leur démarrage manuel ne perturbe en rien les éventuelles planifications configurées et permet de les exécuter immédiatement. Après avoir sélectionné l'option Exécuter les tâches en bloc, cliquez sur Exécuter pour démarrer les tâches en bloc manuellement.

Pour planifier des tâches en bloc (page 366) en vue de les exécuter régulièrement, utilisez la fonction de récurrence. Après avoir sélectionné l'option Exécuter les tâches en bloc, sélectionnez Planifier un nouveau job et choisissez des options.

Le bouton Aperçu permet de voir les objets qui seront affectés par les tâches en bloc avant de démarrer ces dernières.

Remarque : Si votre ensemble de tâches en bloc compte 500 objets, le système crée 500 tâches imbriquées (une par objet). Pour des raisons de performances, il est conseillé de planifier les tâches en bloc portant sur de vastes ensembles.

Onglet Récurrence

Utilisez cet onglet pour planifier votre job. Cet onglet comporte les champs suivants.

Exécuter

Permet d'exécuter le job immédiatement.

Planifier un nouveau job

Permet de planifier un nouveau job.

Modifier le job actuel

Spécifie que vous voulez modifier un job existant.

Remarque : Ce champ apparaît uniquement si un job a déjà été planifié pour cette tâche.

Nom du job

Spécifie le nom du job que vous souhaitez créer ou modifier.

Fuseau horaire

Spécifie le fuseau horaire du serveur.

Remarque : Si votre fuseau horaire est différent de celui du serveur, une liste déroulante permet de sélectionner votre fuseau horaire ou celui du serveur lorsque vous planifiez un nouveau job. Vous ne pouvez pas changer le fuseau horaire lorsque vous modifiez un job existant.

Planification quotidienne

Indique que le job se répète régulièrement après un certain nombre de jours.

Tous les (nombre) jours

Définit le nombre de jours s'écoulant entre deux exécutions du job.

Planification hebdomadaire

Spécifie que le job est exécuté un ou plusieurs jours spécifiques de la semaine, à une heure précise.

Jour de la semaine

Spécifie le ou les jours de la semaine où le job est exécuté.

Planification mensuelle

Spécifie un jour de la semaine ou du mois où le job s'exécute selon une base mensuelle.

Planification annuelle

Spécifie un jour de la semaine ou du mois où le job s'exécute selon une base annuelle.

Planification avancée

Spécifie les informations de planification supplémentaires.

Expression Cron

Pour obtenir des informations sur le remplissage de ce champ, reportez-vous à l'adresse suivante :

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Heure d'exécution

Spécifie l'heure, au format 24 heures, à laquelle le job est exécuté. Par exemple, 14:15.

Vérification de la progression des tâches en bloc

Vous pouvez vérifier la progression des tâches en bloc à l'aide des méthodes suivantes :

- Affichage du statut dans la section d'affichage des tâches soumises

  La fenêtre Afficher les tâches soumises indique un récapitulatif des opérations en bloc. Le récapitulatif inclut le nombre total de tâches, le nombre de tâches terminées et le nombre de tâches restantes. Le récapitulatif fournit également des informations sur le nombre de tâches avec les états Terminé, En cours et Audit.

- Réception de courriels de notification envoyés à l'issue d'une opération en bloc

Récupération de tâches en bloc

Si un échec survient durant l'exécution d'un événement, le principal événement de tâches en bloc indique Echec. Vous pouvez soumettre de nouveau l'événement de tâches en bloc (via l'option Afficher les tâches soumises) de manière à ce que le système redémarre l'ensemble des tâches à l'endroit où l'échec s'est produit.

Cas d'utilisation : modifications d'utilisateurs en bloc

Imaginons que vous souhaitiez effectuer un changement majeur de manière à ce que tous les utilisateurs du service Ventes figurent désormais dans le service Achats.

1. Sous l'onglet Profil des tâches en bloc, créez une définition de tâches en bloc nommée Changer en Achats.
2. Définissez le type d'objet sur Utilisateur.
3. Sélectionnez Modifier un utilisateur comme tâche à exécuter.
4. Cliquez sur Attributs et définissez la valeur du service sur "Achats".

5. Sous l'onglet Ensemble, spécifiez "Service EGAL A Ventes".
6. Sélectionnez Exécuter les tâches en bloc pour appliquer la définition immédiatement.

Cas d'utilisation : attributs contenant des dates

Imaginons que vous souhaitiez créer un processus automatisé pour désactiver les utilisateurs temporaires vingt jours avant leur date de résiliation.

1. Sous Tâches en bloc, créez une définition de tâches en bloc nommée Désactiver un contractant.
2. Définissez le type d'objet sur Utilisateur.
3. Définissez la tâche à exécuter comme Désactiver l'utilisateur.
4. Entrez les valeurs suivantes dans le filtre de date.
   - Attribut : Date de résiliation
   - Opérateur : Avant aujourd'hui
   - Disposition : 20

   Vous pouvez ajouter n'importe quel autre attribut dans le filtre d'ensemble, par exemple Type d'employé = Contractant. Dans ce cas, seuls les contractants sont affectés.

Gestion des connexions JDBC

Les informations des rapports CA IdentityMinder peuvent provenir de plusieurs sources et chaque rapport doit être associé à une source de données spécifique, selon les informations à y afficher.

Pour établir différentes sources de données pour la génération de rapports (par exemple, une base de données d'audit ou de persistance des tâches), créez un objet géré par connexion dans CA IdentityMinder. Une fois la connexion créée, vous pouvez associer un rapport à un objet géré par connexion spécifique en modifiant la tâche de rapport et en définissant l'objet de connexion pour le rapport sous l'onglet Rechercher de la tâche de génération de rapports.

Création d'une connexion JDBC

La procédure ci-après permet de spécifier les détails de connexion dans CA IdentityMinder.

Pour créer une connexion JDBC :

1. Cliquez sur Système, Gestion des connexions JDBC, Créer une connexion JDBC.
2. Créez un objet de connexion ou choisissez un objet de connexion basé sur une source de données JNDI.
3. Renseignez tous les champs nécessaires, puis cliquez sur Soumettre.

   Une connexion JDBC est créée.

Gestionnaires d'attributs logiques

Les attributs logiques de CA IdentityMinder permettent d'afficher les attributs de magasins d'utilisateurs, appelés attributs physiques, dans un format convivial, sur des fenêtres de tâches. Les administrateurs de CA IdentityMinder utilisent les fenêtres de tâches pour exécuter des fonctions dans CA IdentityMinder. Les attributs logiques n'existent pas dans un magasin d'utilisateurs. En général, ils représentent un ou plusieurs attributs physiques pour simplifier la présentation. Par exemple, l'attribut logique Date peut représenter les attributs physiques Mois, Jour et Année.

Les attributs logiques sont traités par des gestionnaires d'attributs logiques : il s'agit d'objets Java écrits à l'aide de l'API d'attribut logique. (Voir le *Manuel de programmation pour Java*.) Par exemple, lorsqu'une fenêtre de tâche s'affiche, un gestionnaire d'attributs logiques peut convertir des données d'attributs physiques provenant du magasin d'utilisateurs en données d'attributs logiques, qui s'affichent sur la fenêtre de tâche. Vous pouvez utiliser des attributs logiques prédéfinis et des gestionnaires d'attributs logiques inclus dans CA IdentityMinder ou en créer de nouveaux à l'aide de l'API d'attribut logique.

Remarque : Pour en savoir plus sur les attributs logiques, voir le *Manuel de programmation pour Java*.

Dans la console d'utilisateur, la catégorie Environnement contient des tâches permettant de gérer les gestionnaires d'attributs logiques. La liste comprend les gestionnaires prédéfinis fournis avec CA IdentityMinder, ainsi que les gestionnaires personnalisés définis sur votre site.

Dans la catégorie de tâche Environnement, vous pouvez effectuer les opérations ci-après.

- Créer un nouveau gestionnaire d'attributs logiques avec CA IdentityMinder
- Copier un gestionnaire

- Supprimer un gestionnaire
- Modifier la configuration d'un gestionnaire existant

Remarque : Pour modifier l'ordre d'exécution des gestionnaires d'attributs logiques, utilisez la console de gestion.

Création d'un gestionnaire d'attributs logiques

Pour créer un gestionnaire d'attributs logiques :

1. Sélectionnez Système, Créer un gestionnaire d'attributs logiques.
2. Dans la fenêtre Créer un gestionnaire d'attributs logiques, sélectionnez Créer un gestionnaire d'attributs logiques standard, puis cliquez sur OK.
3. Dans la fenêtre Créer un gestionnaire d'attributs logiques, configurez les paramètres du gestionnaire d'attributs logiques.

   Pour une description de chaque champ, cliquez sur le lien Aide de cette fenêtre.
4. Cliquez sur Soumettre.

   Le gestionnaire est ajouté à la liste des gestionnaires sur la fenêtre Gestionnaires d'attributs logiques.

Remarque : Il est inutile de redémarrer le serveur d'applications après avoir configuré des gestionnaires d'attributs logiques à l'aide de la console d'utilisateur.

Copie d'un gestionnaire d'attributs logiques

Pour copier un gestionnaire d'attributs logiques :

1. Sélectionnez Système, Créer un gestionnaire d'attributs logiques.
2. Dans la fenêtre Créer un gestionnaire d'attributs logiques, sélectionnez Créer la copie d'une définition de gestionnaire d'attributs logiques, puis cliquez sur Rechercher.
3. Sélectionnez un gestionnaire d'attributs logiques (par exemple, ConfirmPasswordHandler), puis cliquez sur OK.

4. Dans la fenêtre Créer un gestionnaire d'attributs logiques, configurez les paramètres du gestionnaire d'attributs logiques.

   Pour une description de chaque champ, cliquez sur le lien Aide de cette fenêtre.

5. Cliquez sur Soumettre.

   Le gestionnaire est ajouté à la liste des gestionnaires sur la fenêtre Gestionnaires d'attributs logiques.

Remarque : Il est inutile de redémarrer le serveur d'applications après avoir configuré des gestionnaires d'attributs logiques à l'aide de la console d'utilisateur.

Création d'un gestionnaire d'attributs logiques ForgottenPasswordHandler

Le gestionnaire d'attributs logiques ForgottenPasswordHandler utilise des attributs logiques distincts pour les éléments ci-après.

- Configuration
- Questions et réponses d'exécution

Pour créer un gestionnaire d'attributs logiques ForgottenPasswordHandler :

1. Sélectionnez Système, Créer un gestionnaire d'attributs logiques.
2. Dans la fenêtre Créer un gestionnaire d'attributs logiques, sélectionnez Créer un gestionnaire d'attributs logiques standard, puis cliquez sur Rechercher.
3. Sélectionnez le gestionnaire ForgottenPasswordHandler et cliquez sur OK.
4. Dans la fenêtre Créer un gestionnaire d'attributs logiques : ForgottenPasswordHandler, configurez les paramètres pour le gestionnaire d'attributs logiques.

   Pour une description de chaque champ, cliquez sur le lien Aide de cette fenêtre.

5. Cliquez sur Soumettre.

   Le gestionnaire est ajouté à la liste des gestionnaires sur la fenêtre Gestionnaires d'attributs logiques.

Remarque : Il est inutile de redémarrer le serveur d'applications après avoir configuré des gestionnaires d'attributs logiques à l'aide de la console d'utilisateur.

Suppression d'un gestionnaire d'attributs logiques

Pour supprimer un gestionnaire d'attributs logiques :

1. Sélectionnez Système, Supprimer le gestionnaire d'attributs logiques.
2. Dans la fenêtre Supprimer un gestionnaire d'attributs logiques, cochez la case à gauche de chaque attribut logique à supprimer.

3. Cliquez sur Sélectionner.

   CA IdentityMinder affiche un message de confirmation.

4. Cliquez sur Oui pour confirmer la suppression.

Modification d'un gestionnaire d'attributs logiques

Pour modifier un gestionnaire d'attributs logiques :

1. Sélectionnez Système, Modifier le gestionnaire d'attributs logiques**.**
2. Dans la fenêtre Modifier un gestionnaire d'attributs logiques, sélectionnez le gestionnaire que vous souhaitez modifier, puis cliquez sur Sélectionner.
3. Sélectionnez un gestionnaire d'attributs logiques (par exemple, ConfirmPasswordHandler), puis cliquez sur OK.
4. Dans la fenêtre Modifier le gestionnaire d'attributs logiques, configurez les paramètres du gestionnaire d'attributs logiques.

   Pour une description de chaque champ, cliquez sur le lien Aide de cette fenêtre.

5. Cliquez sur Soumettre.

Remarque : Il est inutile de redémarrer le serveur d'applications après avoir configuré des gestionnaires d'attributs logiques à l'aide de la console d'utilisateur.

Affichage d'un gestionnaire d'attributs logiques

Pour afficher un gestionnaire d'attributs logiques :

1. Sélectionnez Système, Afficher le gestionnaire d'attributs logiques**.**
2. Dans la fenêtre Afficher le gestionnaire d'attributs logiques, sélectionnez le gestionnaire que vous souhaitez afficher, puis cliquez sur Sélectionner.
3. Affichez les propriétés du gestionnaire d'attributs logiques, puis cliquez sur Fermer.

Données des boîtes de sélection

Vous pouvez spécifier les options disponibles dans les champs suivants :

- Case à cocher : sélection multiple
- Liste déroulante
- Liste modifiable déroulante
- Sélection multiple
- Sélecteur d'options

- Sélecteur modifiable d'options
- Sélection unique avec bouton d'option
- Sélection unique

Ces options sont stockées dans des fichiers XML de données de boîtes de sélection. Par exemple, vous pouvez utiliser les fichiers XML de données de boîtes de sélection pour remplir des options dans une case déroulante de Ville ou d'Etat sur un onglet Profil pour la tâche Créer un utilisateur.

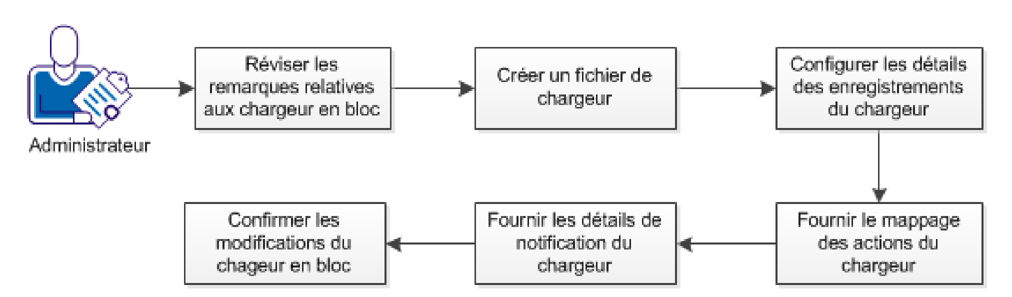
Vous pouvez également utiliser les fichiers XML de données de boîtes de sélection pour définir une dépendance entre deux champs d'une tâche d'administration. Par exemple, les options qui sont disponibles dans le champ Ville peuvent dépendre d'une option choisie par l'utilisateur dans le champ Etat.

Remarque : Pour plus d'informations sur les données des boîtes de sélection, reportez-vous au *manuel de conception de la console d'utilisateur (en anglais).*

Procédure d'ajout d'utilisateurs avec un fichier de chargeur

Vous pouvez utiliser l'onglet Chargeur en bloc pour charger les fichiers d'insertion qui sont utilisés pour manipuler de grands nombres d'objets gérés simultanément. Par exemple, vous pouvez créer 1 000 utilisateurs manuellement dans le système ou vous pouvez utiliser le chargeur en bloc. La tâche Chargeur en bloc peut également être mappée vers un processus de flux de travaux.

Le client de chargement en bloc est un utilitaire de ligne de commande disponible pour le traitement par lots. Il est recommandé d'utiliser le client de chargement en bloc si votre environnement se trouve dans un cluster (à des fins d'équilibrage de charge). Le client de chargement en bloc est accessible sur le média des composants de provisionnement.



Procédez comme suit:

1. Révisez les remarques relatives au chargeur en bloc (page 589).
2. Créez un fichier de chargeur CSV ou XLS (page 590) et chargez-le.

3. Configurez les détails des enregistrements du chargeur (page 592).

   L'onglet Détails des enregistrements du chargeur permet de spécifier les champs d'action et d'identifiant dans le fichier de chargeur.

4. Indiquez le mappage des actions du chargeur (page 592).

   L'onglet Mappage des actions du chargeur permet de sélectionner l'objet principal et de spécifier la tâche à exécuter pour l'action appliquée à un objet.

5. Fournissez les détails de notification du chargeur (page 593).

   L'onglet Détails de la notification du chargeur vous permet de sélectionner des utilisateurs pour certifier les modifications des tâches du chargeur en bloc.

6. Confirmez et modifiez la progression des modifications des tâches du chargeur en bloc (page 594).

Remarques relatives au chargeur en bloc

Vous pouvez utiliser l'onglet Chargeur en bloc pour charger les fichiers d'insertion qui sont utilisés pour manipuler de grands nombres d'objets gérés simultanément. Tenez compte des remarques suivantes lors de l'utilisation du chargeur en bloc :

- Planifiez les chargements en bloc volumineux pendant les périodes creuses, telles que la nuit. Les chargements en bloc volumineux peuvent affecter les performances. Dans certains cas, un chargement en bloc qui inclut de nombreuses sous-tâches peut empêcher les tâches soumises par les utilisateurs de s'exécuter tant que le chargement en bloc n'est pas terminé.
- Si le serveur tombe en panne pendant une tâche dont l'exécution est longue, telle que le chargement d'un grand nombre d'objets, vous pouvez relancer la tâche dans l'onglet Afficher les tâches soumises. Quand la tâche redémarre, elle commence par le dernier enregistrement réussi.
- L'utilisation d'un référentiel d'utilisateurs LDAP avec Solaris peut entraîner un blocage du chargeur en bloc au cours de l'importation. Pour résoudre ce problème, consultez la rubrique relative à la spécification de paramètres de connexion LDAP dans le *manuel de configuration* et appliquez les paramètres décrits ici.
- Si vous utilisez le chargeur en bloc pour importer un grand nombre d'utilisateurs, vous pouvez recevoir des exceptions de mémoire insuffisante. Pour résoudre ce problème, ajustez les paramètres de taille de segment de mémoire suivants :
  - -Xmx
  - -XX:maxPermSize

    Remarque : Pour plus d'informations sur le réglage des paramètres de mémoire, consultez la documentation du serveur d'applications.

- L'utilisation du chargeur en bloc pour manipuler de nombreux objets gérés, par exemple pour créer de nombreux utilisateurs, peut affecter les performances. Pour améliorer les performances, tenez compte des recommandations suivantes :
  - Divisez les fichiers CSV volumineux en plusieurs petits fichiers lorsque vous utilisez la console d'utilisateur pour effectuer des chargements en bloc. Par exemple, le chargement de dix blocs de 10 000 utilisateurs sera plus rapide qu'un seul chargement de 100 000 utilisateurs.
  - Limitez le nombre de tâches des utilisateurs chargés du chargement en bloc. Par exemple, les performances sont améliorées lorsque l'administrateur qui lance le chargement en bloc se charge uniquement de quelques tâches. Si l'administrateur doit se charger de nombreuses tâches, CA IdentityMinder doit procéder à de contrôles plus étendus des autorisations, ce qui peut affecter les performances.
  - Limitez le nombre de stratégies Policy Xpress associées aux modifications en bloc, qui impliquent le provisionnement. Vous pouvez également créer des stratégies Policy Xpress simples qui affectent moins les performances que les stratégies complexes lors de l'opération de chargement en bloc.
  - Vérifiez que vos ressources système sont suffisantes.

Créer un fichier d'insertion.

Un fichier de chargeur en bloc est utilisé pour automatiser des actions répétées sur un grand nombre d'objets gérés. Lorsque vous chargez un fichier de chargeur, le système analyse et lit le fichier de chargeur.

Ce fichier doit avoir une extension CSV ou XLS et les propriétés ci-après.

- Le fichier doit contenir une ligne d'en-tête spécifiant les attributs physiques, les attributs logiques ou les noms d'attribut connus d'un objet géré.
- La ligne d'en-tête doit inclure une colonne qui indique l'action à entreprendre sur les enregistrements.
- Chaque ligne du fichier de chargeur s'appelle un enregistrement. Les enregistrements contiennent les valeurs de chacun des attributs spécifiés par la ligne d'en-tête. Les options ci-après représentent des valeurs acceptables pour un attribut.
  - Valeur : l'attribut est défini sur la valeur spécifiée.
  - Valeur;Valeur;Valeur;... : l'attribut est défini sur l'attribut à valeurs multiples que vous spécifiez.

- ' ' (vide) : l'attribut n'est pas modifié.
- NUL : l'attribut est supprimé. La séquence de suppression est définie par défaut sur la valeur NUL. Elle peut être modifiée dans la fenêtre Recherche du chargement de fichiers du chargeur en bloc.

Remarque : Pour utiliser un dièse (#) dans le fichier du chargeur, incluez-le entre guillemets ; par exemple, utilisateur#1 doit être spécifié comme "utilisateur#1".

Important : Le fichier du chargeur doit être enregistré avec le codage UTF-8.

Fichier d'exemple de chargeur pour la création d'utilisateurs

Ce fichier de chargeur d'exemple crée des utilisateurs avec certains attributs requis.

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

Dans les codes précédents, le fichier de chargeur a les propriétés ci-après.

En-tête

La première ligne du code est la ligne d'en-tête. La ligne d'en-tête comporte des attributs physiques ou des attributs réservés pour l'objet géré Utilisateur.

Action

La colonne Action identifie la tâche à effectuer pour chaque enregistrement. Par exemple, le fichier précédent spécifie qu'une action "créer" doit être effectuée sur le prénom John.

Fichier d'exemple de chargeur pour l'activation d'utilisateurs

Ce fichier d'exemple de chargeur change la valeur de l'attribut logique |enabled|. Vous spécifiez l'attribut logique dans l'en-tête et la valeur (dans ce cas, true ou false) dans chaque entrée d'utilisateur dans le fichier.

```
action,%USER_ID%,|enable|

MODIFY,user1,false

MODIFY,user2,true
```

Onglet Détails des enregistrements du chargeur

L'onglet Détails des enregistrements du chargeur affiche un bref aperçu des enregistrements disponibles dans votre fichier de chargeur. Le tableau d'aperçu affiche 5 enregistrements maximum. Il permet aux utilisateurs de savoir s'ils chargent le bon fichier. Cet onglet permet également d'identifier l'action à effectuer sur les objets gérés spécifiés dans votre fichier du chargeur. Vous devez renseigner les champs suivants :

Quel champ représente l'action à réaliser sur l'objet ?

Identifie les champs du fichier du chargeur qui indiquent l'action à effectuer sur les objets gérés. Par exemple, vous pouvez utiliser un fichier du chargeur avec un champ "action" qui prend les valeurs Créer, Modifier et Supprimer. Vous devez mapper chacune de ces actions sur une tâche d'administration dans Mappage des actions du chargeur (page 592).

Quel champ sera utilisé pour identifier l'objet de manière unique ?

Identifie le champ du fichier du chargeur qui peut identifier de manière unique l'objet principal.

Remarque : Si le fichier du chargeur comporte une ligne d'en-tête non valide, les enregistrements du fichier du chargeur ne s'affichent pas sous l'onglet Détails des enregistrements du chargeur. Si des lignes d'en-tête sont non valides, sélectionnez un autre fichier du chargeur. Si le fichier du chargeur contient des enregistrements non valides, l'état détaillé du chargement apparaît dans Afficher les tâches soumises dans l'onglet Système.

Onglet Mappage des actions du chargeur

L'onglet Mappage des actions du chargeur permet de sélectionner un objet principal sur lequel effectuer les actions spécifiées dans le fichier du chargeur. Vous devez également mapper les actions du fichier du chargeur vers les tâches d'administration pour l'objet principal sélectionné.

Quel est l'objet principal ?

Identifie l'objet principal qu'CA IdentityMinder manipulera à l'aide du fichier du chargeur. Vous pouvez sélectionner l'un des objets principaux suivants.

- Utilisateur
- Groupes
- Organisation

Sélectionner une tâche à exécuter pour l'action

Identifie les tâches d'administration à effectuer pour chaque action spécifiée par le fichier du chargeur, telles que les tâches Supprimer ou Modifier.

Remarque : Vous devez mapper toutes les actions du fichier du chargeur vers une tâche d'administration. De même, les tâches d'administration affichées dans ce champ dépendent de l'objet principal sélectionné. Par exemple, si vous sélectionnez "Utilisateur" comme objet principal, seules les tâches d'administration relatives à "Utilisateur" s'affichent.

Sélectionner une tâche pour l'objet non existant pour l'action

Identifie les autres tâches d'administration, telles que la tâche Créer, à exécuter pour une action spécifiée dans le fichier du chargeur si l'objet géré n'existe pas encore dans CA IdentityMinder.

Onglet Détails de la notification du chargeur

Important : Par défaut, cet onglet n'est pas inclus dans l'assistant du chargeur en bloc. Vous devez l'ajouter manuellement en modifiant la tâche du chargeur en bloc et en ajoutant l'onglet Détails de la notification du chargeur. Cet onglet nécessite également que vous activiez le flux de travaux dans l'environnement.

L'onglet Détails de la notification du chargeur vous permet de sélectionner les gestionnaires de certifications pour la tâche du chargeur en bloc. Lorsqu'une tâche du chargeur en bloc se termine, CA IdentityMinder crée une notification du chargeur en bloc pour tous les gestionnaires de certifications configurés pour la tâche. Cette notification s'affiche dans l'onglet Accueil, sous Notifications du chargeur en bloc. Si vous cliquez sur la notification, des informations s'affichent pour les tâches lancées par l'opération de chargement en bloc. Les gestionnaires de certifications peuvent alors examiner les modifications détaillées dans les notifications et en tenir compte.

Remarque : Pour fournir une liste des gestionnaires de certifications, utilisez l'un des outils de résolution de participants disponibles dans la liste déroulante. Pour plus d'informations sur les outils de résolution de participants, consultez la section Flux de travaux de ce manuel.

Confirmation des modifications apportées par la tâche du chargeur en bloc

Les notifications du chargeur en bloc contiennent des informations sur toutes les modifications lancées par la tâche du chargeur en bloc. Les gestionnaires de certifications peuvent examiner les modifications lancées par une tâche du chargeur en bloc.

Pour examiner les modifications apportées par une tâche du chargeur en bloc

1. Connectez-vous à la console d'utilisateur en tant qu'utilisateur répertorié comme gestionnaire de certifications pour une tâche du chargeur en bloc.
2. Accédez aux options Accueil, Afficher mes notifications du chargeur en bloc.
3. Sélectionnez la notification du chargeur en bloc que vous souhaitez examiner.

   La fenêtre Gérer les notifications du chargeur en bloc s'affiche et comporte une table répertoriant toutes les modifications de tâche du chargeur en bloc ayant été lancées.

   Sur cet écran, vous pouvez effectuer les opérations suivantes :

   - Pour examiner les détails d'une tâche spécifique relatifs à un objet de création ou de modification, cliquez sur le lien hypertexte situé sous la colonne Description.
   - En cas de violation de la conformité, ou si vous souhaitez supprimer un rôle ajouté à un utilisateur, vous pouvez modifier l'utilisateur directement à partir de la fenêtre de notification en cliquant sur l'icône Modifier à côté de l'ID d'utilisateur.
   - Pour examiner les rôles ajoutés à un utilisateur, cliquez sur le lien hypertexte sous la colonne Demandes d'affectation de rôles associée à l'ID d'utilisateur.

4. Après avoir examiné toutes les modifications apportées à un objet spécifique, sélectionnez la case à cocher Confirmer pour cet objet.
5. Après avoir confirmé les modifications, cliquez sur Confirmer pour supprimer toutes les notifications de modification de la liste.

   Remarque : Vous pouvez sélectionner l'option Tout confirmer afin de confirmer toutes les modifications dans une notification du chargeur en bloc. Ainsi, la notification du chargeur en bloc est supprimée de l'onglet Accueil. Vous pouvez également sélectionner la case à cocher située en haut de la colonne Confirmer afin de sélectionner simultanément toutes les notifications de modification de la fenêtre et confirmer les modifications fenêtre par fenêtre.

   Lorsque toutes les modifications d'utilisateurs associées à une tâche du chargeur en bloc sont confirmées, la notification du chargeur en bloc disparaît de l'onglet Accueil.

Configuration des courriels de notification pour des tâches de chargeur en bloc

Dans certains environnements, les courriels de notification des opérations en bloc sont configurés par défaut. Pour vérifier si les courriels de notification des opérations en bloc sont configurées dans votre système, cliquez sur Système, Courriel, Afficher un courriel et recherchez le terme bloc.

Si aucune notification par courriel n'est configurée dans votre environnement, configurez le courriel qui est envoyé à l'issue d'une opération en bloc.

Procédez comme suit:

1. Dans la console d'utilisateur, cliquez sur Système, Courriel, Créer un courriel.
2. Dans l'onglet Profil, renseignez les champs requis.
3. Dans l'onglet Planification de l'envoi, effectuez les étapes suivantes :
   a. Sélectionnez Fin de la tâche dans le premier champ.
   b. Sélectionnez Chargeur en bloc dans le deuxième champ.
4. Remplissez les onglets Destinataires et Contenu, puis cliquez sur Soumettre.

   Les notifications par courriel sont configurées pour les tâches du chargeur en bloc.

Planification d'une tâche Chargeur en bloc

Vous pouvez planifier la tâche Chargeur en bloc dans le système. Pour planifier la tâche Chargeur en bloc, ajoutez un onglet Planificateur (page 70) à la tâche.

Modification du fichier d'analyse pour le chargeur en bloc

Pour modifier l'analyseur utilisé pour analyser les fichiers de chargeur, configurez la tâche d'administration correspondante.

Pour modifier la tâche d'administration du chargeur en bloc

1. Cliquez sur Rôles et tâches, Tâches d'administration, puis Modifier la tâche d'administration.
2. Recherchez la tâche Chargeur en bloc.
3. Sélectionnez la tâche Chargeur en bloc, puis cliquez sur Sélectionner.
4. Sélectionnez l'onglet Recherche dans la tâche Chargeur en bloc.

5. Cliquez sur Parcourir pour localiser les fenêtres de recherche.

   La liste des fenêtres de recherche disponibles s'affiche.

6. Sélectionnez une fenêtre de recherche, puis cliquez sur Modifier.

   La fenêtre de détails de la recherche apparaît.

7. (Facultatif) Modifiez le nom complet de l'analyseur.

   Le nom complet de l'analyseur doit correspondre au nom de votre fichier d'analyse.

   Remarque : Pour plus d'informations sur la création d'un analyseur CSV personnalisé, reportez-vous à l'outil Javadoc associé à la classe FeederParser. Si vous utilisez JBoss comme serveur d'applications et créez un analyseur personnalisé, le fichier d'analyseur personnalisé doit se trouver dans le répertoire iam_im.ear/user_console_war/WEB-INF/classes.

8. Cliquez sur OK.

Support du service Web du chargeur en bloc

Le chargeur en bloc dispose d'une API de service Web qui peut être appelé à l'aide d'une interface TEWS (Task Execution Web Service) de CA IdentityMinder. TEWS permet aux applications clientes de soumettre des tâches à distance à CA IdentityMinder pour leur exécution. Cette interface applique les normes ouvertes WSDL et SOAP pour fournir un accès à distance à CA IdentityMinder.

CA IdentityMinder inclut des exemples de clients Java qui illustrent l'appel du chargeur en bloc en tant que service Web. Les exemples Java se trouvent dans le fichier source suivant :

outils_admin\samples\WebService\Axis\optional\ObjectsFeeder.java

Les échantillons de données et la documentation d'appel du chargeur en bloc en tant que service Web se trouvent dans le répertoire suivant :

outils_admin\samples\Feeder\

Remarque : Pour plus d'informations, reportez-vous au manuel *Programming Guide for Java*.

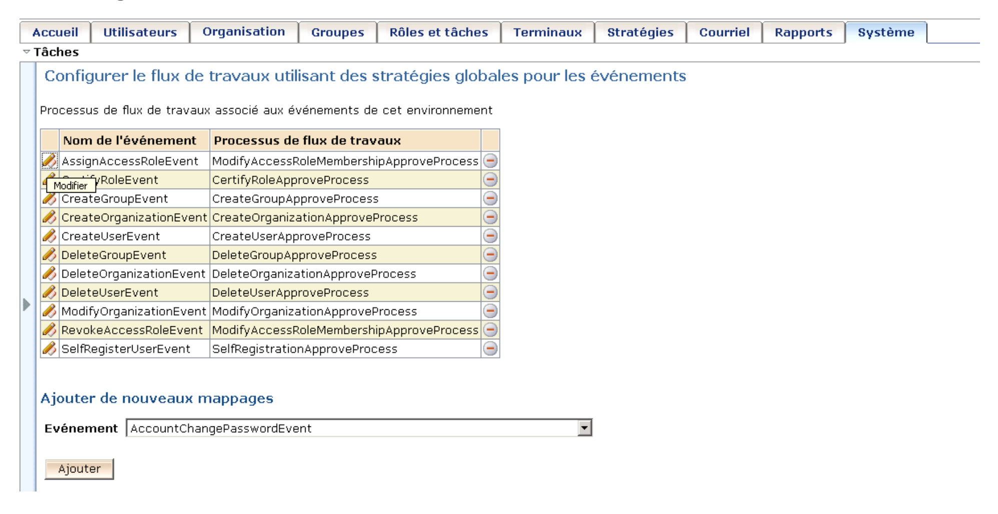
Configuration de la fenêtre de tâche d'attributs de corrélation

Utilisez la fenêtre de configuration de tâche d'attributs de corrélation pour configurer des règles de corrélation pour l'environnement.

CA IdentityMinder lit les paramètres de configuration dans la mémoire et synchronise périodiquement la version de la mémoire avec la version de base de données du DSA commun. Les attributs de corrélation étant propres au client hébergé spécifique, le serveur de provisionnement lit les attributs de corrélation à partir du DSA de client hébergé correspondant pendant les opérations d'exploration et de corrélation. Les règles de corrélation mises à jour prennent effet immédiatement sans attendre l'heure de mise à jour des paramètres.

Fenêtre de tâche Configurer le flux de travaux utilisant des stratégies globales pour les événements

La tâche Configurer le flux de travaux utilisant des stratégies globales pour les événements permet à un administrateur de configurer un flux de travaux utilisant ou non des stratégies pour tous les événements de l'environnement actuel. Si vous cliquez sur la tâche, vous voyez le mappage des événements par défaut vers les définitions de processus de flux de travaux. Chaque mappage d'événement peut être modifié ou supprimé et il est possible d'en ajouter de nouveaux pour les événements qui n'ont pas été configurés.



Les champs de cette fenêtre sont répertoriés ci-dessous.

Processus de flux de travaux associé aux événements de cet environnement

Spécifie les processus de flux de travaux associés aux stratégies d'approbation.

Ajouter de nouveaux mappages

Spécifie une stratégie d'approbation à mapper vers un processus de flux de travaux.

Bouton Ajouter

Ajoute le nouveau mappage.

L'ajout ou la modification d'un mappage ouvre la fenêtre Mappage du flux de travaux qui permet de sélectionner les mappages de processus et les stratégies d'approbation. Le comportement est identique à la configuration de flux de travaux de niveau événement. Si vous cliquez sur le bouton Ajouter de la page Mappage du flux de travaux, une autre page s'affiche et vous permet de configurer une stratégie d'approbation.

Informations complémentaires

Configuration du flux de travaux utilisant des stratégies pour les événements (page 484)
Configuration d'une stratégie d'approbation (page 487)

Statut des tâches dans CA IdentityMinder

Les administrateurs peuvent suivre le statut des tâches CA IdentityMinder après leur soumission pour le traitement. CA IdentityMinder permet d'afficher l'état des tâches de différentes façons :

- **Onglet Afficher les tâches soumises**

  Cet onglet vous permet de rechercher et d'afficher les tâches CA IdentityMinder soumises pour le traitement.

  Les administrateurs peuvent voir des détails de haute qualité des tâches ou afficher des niveaux supplémentaires de détails

  L'onglet Afficher les tâches soumises est inclus dans deux tâches par défaut :

  - Afficher mes tâches soumises

    Permet aux administrateurs de rechercher et afficher les informations sur les tâches qu'ils ont soumises au traitement.

  - Affichage des tâches soumises

    Permet aux administrateurs de rechercher et afficher les informations sur les tâches que d'autres administrateurs ont soumises au traitement.

- **Onglet Historique de l'utilisateur**

  Cet onglet, que vous pouvez ajouter à d'autres tâches, telles que les tâches Afficher ou Modifier un utilisateur, permet aux administrateurs d'afficher les informations suivantes pour un utilisateur sélectionné :

  - Tâches effectuées sur l'utilisateur
  - Tâches effectuées par l'utilisateur
  - Approbations des flux de travaux par l'utilisateur

- **Rapports**

  Les rapports CA IdentityMinder permettent d'afficher l'état actuel d'un environnement CA IdentityMinder. Vous pouvez utiliser ces informations pour vous assurer de la conformité avec les stratégies métiers internes ou les réglementations externes.

  La génération de rapports fournit des informations supplémentaires sur la configuration et l'utilisation des rapports.

- **Journaux**

  Affiche les informations sur tous les composants d'une installation CA IdentityMinder et fournit les détails de toutes les opérations dans CA IdentityMinder.

  Pour plus d'informations sur les journaux de CA IdentityMinder, reportez-vous au *Manuel de configuration*.

Détermination de l'état de la tâche par Identity Manager

Une *tâche* est une fonction administrative qu'un utilisateur peut effectuer dans CA IdentityMinder. Les tâches comprennent les *événements* et les actions que CA IdentityMinder effectue pour terminer la tâche. Une tâche peut inclure plusieurs événements. Par exemple, la tâche Créer un utilisateur peut inclure des événements, qui peuvent créer le profil de l'utilisateur, ajouter l'utilisateur à un groupe et affecter des rôles.

Les tâches et événements CA IdentityMinder peuvent être associés à un processus de flux de travaux, qui détermine la manière dont CA IdentityMinder effectue les actions requises et d'autres tâches métier personnalisées. Les tâches peuvent aussi être associées à d'autres tâches, appelées tâches imbriquées. Dans ce cas, CA IdentityMinder traite les tâches imbriquées avec la tâche originale.

L'état d'une tâche dépend de l'état des événements associés, processus de flux de travaux, tâches imbriquées et tâches métier personnalisées.

Affichage des tâches soumises

CA IdentityMinder inclut l'option Afficher les tâches soumises qui fournit des informations sur les tâches dans un environnement CA IdentityMinder. Vous pouvez utiliser cette fonctionnalité pour rechercher et afficher des informations générales sur les actions effectuées par CA IdentityMinder. Les fenêtres de détails fournissent des informations complémentaires sur chaque tâche et événement.

Selon le statut de la tâche, vous pouvez utiliser l'option Afficher les tâches soumises pour annuler ou soumettre de nouveau une tâche.

L'onglet Afficher les tâches soumises vous permet de suivre le traitement d'une tâche du début à la fin. Par exemple, si une tâche CA IdentityMinder inclut des affectations de rôles de provisionnement et si cette affectation déclenche la création de comptes sur d'autres systèmes, l'onglet Afficher les tâches soumises affiche tous les détails de la tâche d'origine et des créations de comptes.

La fenêtre Afficher les tâches soumises inclut les détails des opérations effectuées sur le système. Ces opérations peuvent être le résultat d'un événement CA IdentityMinder, tel que EnableUserEvent. Les notifications envoyées par le système sont regroupées sous cet événement. Afficher les tâches soumises affiche un message indiquant que les notifications sont en cours jusqu'à ce que la notification de détail de fin soit envoyée. L'état du message devient alors Terminé.

Par défaut, CA IdentityMinder inclut l'onglet Afficher les tâches soumises dans les deux tâches ci-après.

- Affichage des tâches soumises
- Afficher mes tâches soumises

Recherche de tâches soumises

Suivez les étapes suivantes pour rechercher des tâches soumises.

Pour rechercher des tâches soumises :

1. Cliquez sur Système, Afficher les tâches soumises.

   La page Afficher les tâches soumises apparaît.

2. Spécifiez les critères de recherche, saisissez le nombre de lignes à afficher et cliquez sur Rechercher.

   Les tâches qui remplissent les critères de recherche sont affichées.

   Remarque : Pour plus d'informations sur la spécification des attributs dans les critères de recherche, consultez la section Recherche d'attributs pour l'affichage des tâches soumises (page 601).

Recherche d'attributs pour l'affichage des tâches soumises

Pour vérifier les tâches soumises au traitement, vous pouvez utiliser la fonctionnalité de recherche Afficher les tâches soumises. Vous pouvez rechercher des tâches sur les critères suivants :

Lancé par

Identifie le nom de l'utilisateur ayant lancé la tâche comme critère de recherche. Les recherches sont basées sur le nom d'utilisateur. Pour vérifier que vous avez saisi un nom d'utilisateur valide, utilisez le bouton Valider.

Tâches d'approbation effectuées par

Identifie le nom de l'approbateur de tâche comme critère de recherche. Les recherches sont basées sur le nom d'utilisateur. Pour vérifier que vous avez saisi un nom d'utilisateur valide, utilisez le bouton Valider.

Remarque : Si vous sélectionnez le critère Tâches d'approbation effectuées par, le critère Afficher les tâches d'approbation est également activé par défaut.

Nom de la tâche

Identifie le nom de la tâche comme critère de recherche. Vous pouvez affiner la recherche en spécifiant des conditions telles que Egal à, Contient, Commence par ou Finit par la valeur du champ Nom de la tâche. Par exemple, vous pouvez spécifier le critère de recherche : Nom de la tâche est égal à Créer un utilisateur, en sélectionnant la condition Egale à et en saisissant Créer un utilisateur dans le champ de texte.

Statut de la tâche

Identifie le statut de la tâche comme critère de recherche. Vous pouvez sélectionner le statut de la tâche en activant l'option Statut de la tâche égal à et en sélectionnant la condition. Vous pouvez affiner la recherche en vous basant sur les conditions suivantes :

- Terminé
- En cours
- Echec
- Rejeté
- Incomplet
- Interrompu
- Planifié

Remarque : Pour plus d'information, reportez-vous à la section Description de l'état de la tâche (page 603).

Priorité des tâches

Identifie la priorité de la tâche comme critère de recherche. Vous pouvez sélectionner la priorité de la tâche en activant Priorité de la tâche égale à et en sélectionnant la condition. Vous pouvez affiner la recherche en vous basant sur les conditions suivantes :

Faible

Spécifie que vous pouvez rechercher des tâches ayant une priorité faible.

Moyenne

Spécifie que vous pouvez rechercher des tâches ayant une priorité moyenne

Elevée

Spécifie que vous pouvez rechercher des tâches ayant une priorité élevée

Effectué le

Identifie les tâches effectuées sur l'instance de l'objet. Si vous ne sélectionnez pas une instance de l'objet, les tâches qui sont effectuées sur toutes les instances de cet objet seront affichées.

Remarque : Ce champ apparaît uniquement quand le champ Configuration réalisée sur est remplie dans la fenêtre Configurer les tâches soumises Vous utilisez cet écran pour configurer l'onglet Tâches soumises. Pour plus d'informations, reportez-vous à l'aide en ligne pour cette fenêtre

Intervalle de dates

Identifie les dates entre lesquelles vous souhaitez rechercher les tâches soumises. Vous devez remplir les champs A partir de la date et Date de fin.

Afficher les tâches non soumises

Identifie les tâches dont l'état est défini sur Audit. Les tâches à l'origine d'autres tâches, ou les tâches non soumises sont identifiées. Toutes ces tâches seront auditées et affichés si vous sélectionnez cet onglet.

Afficher les tâches d'approbation

Identifie les tâches qui doivent être approuvées dans le cadre d'un flux de travaux.

Rechercher les archives des tâches soumises

Identifie les tâches soumises archivées.

Informations complémentaires :

Description du statut des tâches (page 603)

Description du statut des tâches

Une tâche soumise est définie sur l'un des états décrits ci-après. En fonction de cet état, vous pouvez effectuer des actions telles que l'annulation ou la nouvelle soumission d'une tâche.

Remarque : Pour annuler ou soumettre de nouveau une tâche, vous devez configurer Afficher les tâches soumises pour afficher les boutons Annuler et Resoumettre selon les états des tâches. Pour plus d'informations sur l'annulation et la nouvelle soumission des tâches, reportez-vous à la section Personnalisation de l'onglet Afficher les tâches soumises (page 606).

En cours

Ce statut s'affiche dans l'une des situations suivantes :

- Le flux de travaux est lancé, mais n'est pas terminé.
- Des tâches lancées avant les tâches actuelles, sont en cours.
- Des tâches imbriquées sont lancées, mais ne sont pas terminées.
- L'événement principal est lancé, mais n'est pas terminé.
- Les événements secondaires sont lancés, mais ne sont pas terminés.

Vous pouvez annuler une tâche définie sur cet état.

Remarque : L'annulation d'une tâche annulera toutes les tâches imbriquées et événements non terminés pour la tâche actuelle.

Annulé

Ce statut s'affiche lorsque vous annulez l'une des tâches ou l'un des événements en cours.

Rejeté

Affiché quand CA IdentityMinder rejette un événement ou une tâche qui fait partie d'un processus de flux de travaux. Vous pouvez soumettre de nouveau une tâche rejetée.

Remarque : Quand vous soumettez de nouveau une tâche, CA IdentityMinder soumet de nouveau la totalité des tâches imbriquées et événements qui ont été rejetés.

Incomplet

Ce statut s'affiche lorsque vous annulez certains des événements ou des tâches imbriquées. Vous pouvez soumettre de nouveau une tâche imbriquée ou un événement incomplet.

Terminé

Ce statut s'affiche lorsqu'une tâche est terminée, c'est-à-dire lorsque toutes les tâches imbriquées et événements pour la tâche actuelle sont terminés.

Echec

Ce statut s'affiche lorsqu'une tâche, une tâche imbriquée ou événement imbriqué dans la tâche actuelle ne sont pas valides, c'est-à-dire en cas d'échec de la tâche. Vous pouvez soumettre de nouveau une tâche qui a échoué.

Planifié

Ce statut s'affiche lorsque l'exécution de la tâche est planifiée à une date ultérieure. Vous pouvez annuler une tâche définie sur cet état.

Audité

Affiché quand la tâche actuelle est auditée.

Afficher les détails de la tâche

CA IdentityMinder fournit des détails sur les tâches, comme l'état d'une tâche soumise, les tâches imbriquées et les événements associés à une tâche.

Pour afficher les détails d'une tâche soumise :

1. Cliquez sur l'icône flèche droite, en regard de la tâche sélectionnée, dans l'onglet Afficher les tâches soumises.

   Les détails des tâches s'affichent.

   Remarque : Les événements et les tâches imbriquées (le cas échéant) sont affichés dans la page Détails de la tâche. Vous pouvez afficher les détails de la tâche pour chaque tâche et événement.

2. Cliquez sur Fermer.

   L'onglet Détails de la tâche se ferme et CA IdentityMinder affiche l'onglet Afficher les tâches soumises, avec la liste des tâches.

Affichage des informations de l'événement

CA IdentityMinder fournit des détails sur les événements, comme l'état d'un événement soumis, les attributs d'un événement et toute information supplémentaire sur les événements.

Pour afficher les détails d'un événement soumis :

1. Cliquez sur l'icône flèche droite, en regard d'un événement, dans la page Afficher les détails de la tâche.

   Les détails de l'événement s'affichent.

2. Cliquez sur Fermer.

   La page Détails de l'événement est fermée.

Description de l'état d'événement

Les événements dans CA IdentityMinder peuvent afficher un des états décrits précédemment. En fonction de l'état de l'événement, vous pouvez annuler ou soumettre de nouveau un événement pour son exécution.

Remarque : Pour permettre aux administrateurs d'annuler ou soumettre de nouveau un événement, vous devez configurer Afficher les tâches soumises pour afficher les boutons Annuler et Resoumettre. Quand vous configurez la tâche, vous devez spécifier quels administrateurs peuvent annuler ou soumettre de nouveau les événements. Pour plus d'informations sur l'annulation et une nouvelle soumission des événements, reportez-vous à la section Personnalisation de l'onglet Afficher les tâches soumises (page 606).

En cours

Ce statut s'affiche dans l'une des situations suivantes :

- Des flux de travaux ou des pré-événements sont commencés, en cours ou approuvés.
- CA IdentityMinder exécute l'événement.
- CA IdentityMinder exécute les événements postérieurs.

Vous pouvez annuler un événement dans cet état.

Rejeté

Cet état apparaît lorsque CA IdentityMinder rejette un événement qui fait partie du flux de travaux. Vous pouvez soumettre de nouveau un événement rejeté.

Annulé

Affiché quand vous annulez une des événements en cours. Vous pouvez soumettre de nouveau un événement annulé.

Terminé

Affiché quand un événement est terminé.

Echec

Cet état apparaît lorsque CA IdentityMinder rencontre une exception pendant l'exécution d'un événement. Vous pouvez soumettre de nouveau un événement annulé.

Remarque : Vous ne pouvez pas soumettre de nouveau un événement secondaire si l'événement principal affiche l'état Terminé.

Planifié

Affiché quand l'événement est planifié pour être exécuté à une date ultérieure. Vous pouvez annuler un événement dans cet état.

Audité

Affiché quand l'événement actuel est audité.

Personnalisation de l'onglet Afficher les tâches soumises

Vous pouvez personnaliser l'onglet Afficher les tâches soumises comme suit.

- Spécifiez un nom et une balise de tâche différents.
- Modifiez les propriétés d'affichage par défaut. Dès l'installation, les utilisateurs voient une fenêtre de recherche où ils peuvent saisir des critères qui déterminent les tâches s'affichent dans l'onglet. Vous pouvez configurer l'onglet pour afficher automatiquement les tâches soumises pour un jour en cours, évitant ainsi aux utilisateurs de devoir entrer des critères de recherche.
- Déterminez si les événements d'audit s'affichent dans la page Détails de la tâche.
- Ajoutez une colonne supplémentaire à l'affichage de la tâche.
- Spécifiez les critères d'annulation ou de resoumission des tâches et des événements.

Remarque : Certains détails de tâche et d'événement peuvent inclure des données, telles que des salaires et des mots de passe, qui ne doivent pas s'afficher en texte clair dans l'onglet Afficher les tâches soumises. Vous pouvez masquer ces attributs en spécifiant des paramètres de classification des données lorsque vous définissez des attributs dans le fichier directory.xml. Pour plus d'informations sur le fichier directory.xml, reportez-vous au *manuel de configuration (en anglais)*.

Vous pouvez configurer l'onglet Afficher les tâches soumises en modifiant la tâche d'administration correspondante.

Pour configurer l'onglet Afficher les tâches soumises :

1. Cliquez sur Rôles et Tâches, Tâches d'administration, Modifier les tâches d'administration.

   La page Sélectionner une tâche d'administration s'affiche.

2. Sélectionnez Nom ou Catégorie dans le champ Rechercher une tâche administrative où, entrez la chaîne que vous souhaitez rechercher et cliquez sur Rechercher.

   CA IdentityMinder affiche les tâches d'administration qui répondent à vos critères de recherche.

3. Sélectionnez Afficher les tâches soumises, puis cliquez sur Sélectionner.

   CA IdentityMinder affiche les détails de la tâche pour la tâche d'administration Afficher les tâches soumises.

4. Cliquez sur l'onglet Onglets.

   Les onglets utilisés pour l'onglet Afficher les tâches soumises sont affichés.

5. Cliquez sur l'icône flèche droite pour modifier l'onglet Tâches soumises.

   Les détails de l'onglet s'affichent.

6. Modifiez les champs pour personnaliser l'onglet Afficher les tâches soumises comme nécessaire. Voir les paramètres de configuration pour l'onglet Tâches soumises (page 607).

Paramètres de configuration pour l'onglet tâches soumises.

Utilisez les champs suivants pour modifier l'apparence et la fonctionnalité de l'onglet Afficher les tâches soumises.

Nom

Définit le nom de la tâche.

Balise

Définit un identifiant unique pour la tâche. Il est utilisé pour les URL, des services Web ou des fichiers de propriétés. Il doit être composé de lettres, chiffres ou caractères de soulignement commençant par une lettre ou un caractère de soulignement.

Masquer l'onglet

permet de savoir que l'onglet est visible pour les utilisateurs mais qu'il ne sera pas exécuté. Si vous sélectionnez cette notion, CA IdentityMinder affichera une erreur pour les utilisateurs.

Afficher des listes de tâches de charges

Affiche les tâches qui ont été soumises pendant le jour actuel.

Remarque : Si vous avez activé cette option, les utilisateurs qui cliqueront sur Afficher les tâches soumises verront directement les tâches qui ont été soumises le même jour.

Afficher les événements d'audit

Spécifie si les événements audités sont inclus dans les tâches sur la page Afficher les tâches soumises.

Autorise une colonne personnalisée

Indique si vous pouvez ajouter une colonne personnalisée tableau des tâches que vous pouvez voir dans l'onglet Afficher les tâches soumises et l'onglet Historique de l'utilisateur. Par exemple, vous pouvez ajouter une colonne ID d'utilisateur dans le tableau des tâches, qui est affichée dans l'onglet Historique de l'utilisateur.

En-tête de colonne personnalisé

Indique le nom de la colonne personnalisée'.

Attribut de colonne personnalisée

Indique l'attribut qui sera utilisé pour remplir la colonne personnalisée dans le tableau des tâches. Par exemple, si vous recherchez des tâches qui sont effectuées par des employés d'une organisation, vous pouvez ajouter une colonne pour l'organisation affichant l'organisation pour chacun des employés.

Annuler des événements et des tâches

Identifie les critères d'annulation des tâches ou événements. Vous pouvez définir la portée de ce champ en sélectionnant une des options suivantes :

Le créateur de la tâche doit l'utilisateur actuel.

Identifie que vous pouvez annuler ou resoumettre des tâches ou événements que vous avez créés..

Le créateur de la tâche doit se trouver dans la portée

Identifie que vous pouvez annuler ou resoumettre des tâches qui ont été lancées par d'autres utilisateurs, qui correspondent aux règles de portée pour le rôle d'administrateur, ce qui vous permet d'accéder à l'onglet.

Par exemple, vous avez reçu un rôle de gestionnaire d'utilisateurs, qui inclut l'Affichage des tâches soumises, car vous correspondez aux critères de la règle d'appartenance incluant une portée sur tous les utilisateurs dans l'organisation des employés. Vous pouvez annuler ou resoumettre des tâches soumises par tous les utilisateurs dans l'organisation des employés.

Aucune restriction

Identifie que tous les utilisateurs peuvent annuler ou resoumettre une tâche ou un événement.

Non autorisé

Spécifie qu'aucune tâche ni événement ne peut être annulé ou resoumis.

Resoumettre des tâches et des événements

Identifie les critères de resoumission d'une tâche ou un événement. Vous pouvez définir la portée de ce champ en sélectionnant une des options suivantes :

Le créateur de la tâche doit l'utilisateur actuel.

Identifie que vous pouvez annuler ou resoumettre des tâches ou événements que vous avez créés..

Le créateur de la tâche doit se trouver dans la portée

Identifie que vous pouvez annuler ou resoumettre des tâches qui ont été lancées par d'autres utilisateurs, qui correspondent aux règles de portée pour le rôle d'administrateur, ce qui vous permet d'accéder à l'onglet.

Par exemple, vous avez reçu un rôle de gestionnaire d'utilisateurs, qui inclut l'Affichage des tâches soumises, car vous correspondez aux critères de la règle d'appartenance incluant une portée sur tous les utilisateurs dans l'organisation des employés. Vous pouvez annuler ou resoumettre des tâches soumises par tous les utilisateurs dans l'organisation des employés.

Aucune restriction

Identifie que tous les utilisateurs peuvent annuler ou resoumettre une tâche ou un événement.

Non autorisé

Spécifie qu'aucune tâche ni événement ne peut être annulé ou resoumis.

Onglet Historique de l'utilisateur

L'onglet Historique de l'utilisateur vous permet d'afficher des tâches concernant un utilisateur. Les détails de la tâche qui sont affichés dans cet onglet sont aussi visibles dans l'onglet Afficher les tâches soumises.

Remarque : Vous ne pouvez pas ajouter cet onglet pour créer des tâches, comme Créer un utilisateur.

Vous pouvez utiliser cet onglet pour afficher l'historique des tâches suivantes :

- **Tâches effectuées sur l'utilisateur**

  Affiche toutes les tâches effectuées par l'utilisateur sélectionné.

- **Tâches effectuées par l'utilisateur**

  Affiche toutes les tâches effectuées par l'utilisateur sélectionné.

- **Approbations des flux de travaux par l'utilisateur**

  Affiche toutes les tâches que l'utilisateur a approuvé comme partie du flux de travaux.

Remarque: Le type de tâches que vous pouvez afficher dans cet onglet dépend de la configuration de l'onglet L'onglet Personnaliser l'historique de l'utilisateur (page 611) fournit plus d'informations.

Rechercher des attributs pour afficher l'historique de l'utilisateur

Pour revoir les tâches qui ont été soumises au traitement, vous pouvez utiliser la fonctionnalité de recherche de Afficher les tâches soumises. Vous pouvez rechercher des tâches sur les critères suivants :

Nom de la tâche

Identifie le nom de la tâche comme critère de recherche. Vous pouvez affiner la recherche en spécifiant des conditions comme égal à, contient, commence par ou finit par, avec la valeur du champ Nom de la tâche. Par exemple, vous pouvez spécifier le critère de recherche nom de tâche est égal à Créer un utilisateur en sélectionnant la condition égale à et en saisissant Créer un utilisateur dans le champ de texte.

Etat de la tâche

Identifie l'état de la tâche comme critère de recherche Vous pouvez sélectionner l'état de la tâche en activant "état de la tâche égale à" et en sélectionnant la condition. Vous pouvez affiner la recherche en vous basant sur les conditions suivantes :

- Terminé
- En cours
- Echec
- Rejeté
- Terminé -
- Annulé
- Planifié

Remarque : Pour plus d'information, reportez-vous à la section Description de l'état de la tâche (page 603).

Priorité de la tâche

Identifie la priorité de la tâche comme critère de recherche Vous pouvez sélectionner la priorité de la tâche en activant "priorité de la tâche égale à" et en sélectionnant la condition. Vous pouvez affiner la recherche en vous basant sur les conditions suivantes :

Faible

Spécifie que vous pouvez rechercher des tâches ayant une priorité faible.

Moyen

Spécifie que vous pouvez rechercher des tâches ayant une priorité moyenne

Elevé

Spécifie que vous pouvez rechercher des tâches ayant une priorité élevée

Intervalle de dates

Identifie les dates entre lesquelles vous souhaitez rechercher les tâches soumises. Vous devez fournir les dates A partir de et Jusqu'à.

Personnaliser l'onglet Historique de l'utilisateur

Les administrateurs peuvent personnaliser l'onglet Historique de l'utilisateur de la manière suivante :

- Spécifiez un nom et une balise de tâche différents.
- Modifiez les propriétés d'affichage par défaut. Par défaut, les utilisateurs peuvent introduire des critères déterminant les tâches qui s'afficheront dans l'onglet. Les administrateurs peuvent configurer l'onglet pour afficher les tâches soumises pour un jour en cours automatiquement, ce qui évite aux utilisateurs de devoir saisir le critère de recherche.
- Déterminez si les événements d'audit s'affichent dans la page Détails de la tâche.
- Ajoutez une colonne à l'affichage des tâches.
- Spécifiez les critères d'annulation ou de resoumission des tâches et des événements.

Procédez comme suit:

1. Cliquez sur Rôles et Tâches, Tâches d'administration, Modifier les tâches d'administration.

   La page Sélectionner une tâche d'administration s'affiche.

2. Sélectionnez Nom ou Catégorie dans le champ Rechercher une tâche administrative où, entrez la chaîne que vous souhaitez rechercher et cliquez sur Rechercher.

   CA IdentityMinder affiche les tâches d'administration qui répondent à vos critères de recherche.

3. Sélectionnez la tâche qui inclut l'onglet Historique de l'utilisateur et cliquez sur Sélectionner.

   CA IdentityMinder affiche les détails de la tâche pour la tâche administrative.

4. Cliquez sur l'onglet Onglets.

5. Cliquez sur l'icône Modifier située en regard de l'onglet Historique de l'utilisateur.

   Les détails de l'onglet s'affichent.

6. Modifiez les champs pour personnaliser l'onglet Historique de l'utilisateur.

   Reportez-vous à

Paramètres de configuration pour l'onglet Historique de l'utilisateur.

Utilisez les champs suivants pour modifier l'apparence et la fonctionnalité de l'onglet Historique de l'utilisateur..

Nom

Définit le nom de la tâche.

Balise

Définit un identifiant unique pour la tâche. Il est utilisé pour les URL, des services Web ou des fichiers de propriétés. Il doit être composé de lettres, chiffres ou caractères de soulignement commençant par une lettre ou un caractère de soulignement.

Masquer l'onglet

permet de savoir que l'onglet est visible pour les utilisateurs mais qu'il ne sera pas exécuté. Si vous sélectionnez cette notion, CA IdentityMinder affichera une erreur pour les utilisateurs.

Afficher des listes de tâches de charges

Affiche les tâches qui ont été soumises pendant le jour actuel.

Remarque : Si vous avez activé cette option, les utilisateurs qui cliqueront sur Afficher les tâches soumises verront directement les tâches qui ont été soumises le même jour.

Afficher les événements d'audit

Spécifie si les événements audités sont inclus dans les tâches sur la page Afficher les tâches soumises.

Autorise une colonne personnalisée

Indique si vous pouvez ajouter une colonne personnalisée tableau des tâches que vous pouvez voir dans l'onglet Afficher les tâches soumises et l'onglet Historique de l'utilisateur. Par exemple, vous pouvez ajouter une colonne ID d'utilisateur dans le tableau des tâches, qui est affichée dans l'onglet Historique de l'utilisateur.

En-tête de colonne personnalisé

Indique le nom de la colonne personnalisée'.

Attribut de colonne personnalisée

Indique l'attribut qui sera utilisé pour remplir la colonne personnalisée dans le tableau des tâches. Par exemple, si vous recherchez des tâches qui sont effectuées par des employés d'une organisation, vous pouvez ajouter une colonne pour l'organisation affichant l'organisation pour chacun des employés.

Annuler des événements et des tâches

Identifie les critères d'annulation des tâches ou événements. Vous pouvez définir la portée de ce champ en sélectionnant une des options suivantes :

Le créateur de la tâche doit l'utilisateur actuel.

Identifie que vous pouvez annuler ou resoumettre des tâches ou événements que vous avez créés..

Le créateur de la tâche doit se trouver dans la portée

Identifie que vous pouvez annuler ou resoumettre des tâches qui ont été lancées par d'autres utilisateurs, qui correspondent aux règles de portée pour le rôle d'administrateur, ce qui vous permet d'accéder à l'onglet.

Par exemple, vous avez reçu un rôle de gestionnaire d'utilisateurs, qui inclut l'Affichage des tâches soumises, car vous correspondez aux critères de la règle d'appartenance incluant une portée sur tous les utilisateurs dans l'organisation des employés. Vous pouvez annuler ou resoumettre des tâches soumises par tous les utilisateurs dans l'organisation des employés.

Aucune restriction

Identifie que tous les utilisateurs peuvent annuler ou resoumettre une tâche ou un événement.

Non autorisé

Spécifie qu'aucune tâche ni événement ne peut être annulé ou resoumis.

Resoumettre des tâches et des événements

Identifie les critères de resoumission d'une tâche ou un événement. Vous pouvez définir la portée de ce champ en sélectionnant une des options suivantes :

Le créateur de la tâche doit l'utilisateur actuel.

Identifie que vous pouvez annuler ou resoumettre des tâches ou événements que vous avez créés..

Le créateur de la tâche doit se trouver dans la portée

Identifie que vous pouvez annuler ou resoumettre des tâches qui ont été lancées par d'autres utilisateurs, qui correspondent aux règles de portée pour le rôle d'administrateur, ce qui vous permet d'accéder à l'onglet.

Par exemple, vous avez reçu un rôle de gestionnaire d'utilisateurs, qui inclut l'Affichage des tâches soumises, car vous correspondez aux critères de la règle d'appartenance incluant une portée sur tous les utilisateurs dans l'organisation des employés. Vous pouvez annuler ou resoumettre des tâches soumises par tous les utilisateurs dans l'organisation des employés.

Aucune restriction

Identifie que tous les utilisateurs peuvent annuler ou resoumettre une tâche ou un événement.

Non autorisé

Spécifie qu'aucune tâche ni événement ne peut être annulé ou resoumis.

Afficher les tâches

Détermine les tâches qui apparaissent dans l'onglet Historique de l'utilisateur.

Tâches effectuées sur l'utilisateur

Affiche toutes les tâches effectuées par l'utilisateur sélectionné.

Tâches effectuées par l'utilisateur

Affiche toutes les tâches effectuées par l'utilisateur sélectionné.

Approbations des flux de travaux par l'utilisateur

Affiche toutes les tâches que l'utilisateur a approuvé comme partie du flux de travaux.

La tâche Afficher l'activité de l'utilisateur

L'activité de l'utilisateur est historique des tâches engageant un utilisateur spécifique. Les administrateurs peuvent utiliser la tâche Afficher l'activité de k'utilisateur pour suivre les informations de l'utilisateur<;

- Tâches effectuées sur l'utilisateur
- Tâches effectuées par l'utilisateur
- Approbations des flux de travaux par l'utilisateur

Pour afficher l'activité de l'utilisateur

1. Cliquez sur Utilisateurs, Gérer les utilisateurs, Afficher l'activité de l'utilisateur..

   La boîte de dialogue Sélection de l'utilisateur s'affiche.

2. Rechercher un utilisateur et cliquez sur Sélectionner..

   La fenêtre Afficher l'activité de l'utilisateur apparaît..

Remarque : Pour plus d'informations sur l'activité de l'utilisateur affichée, reportez-vous à l'aide en ligne de la console d'utilisateur.

Nettoyage des tâches soumises

Avec chaque tâche soumise, la performance d'exécution des tâches et des événements ralentit en raison de la croissance de la base de données de persistance des tâches. Le nettoyage des procédures stockées réduit la probabilité que des problèmes de performances ou des défaillances du système surviennent en raison du manque d'espace disque dans la base de données de persistance des tâches. La fonction d'archivage des tâches permet à l'administrateur d'afficher les informations actuelles relatives à la tâche et à l'événement, ainsi que les tâches et les informations supprimées.

Dans la console d'utilisateur, l'administrateur CA IdentityMinder peut planifier des jobs pour effectuer automatiquement la collecte et l'archivage des procédures stockées.

Onglet Récurrence

Utilisez cet onglet pour planifier votre job. Cet onglet comporte les champs suivants.

Exécuter

Permet d'exécuter le job immédiatement.

Planifier un nouveau job

Permet de planifier un nouveau job.

Modifier le job actuel

Spécifie que vous voulez modifier un job existant.

Remarque : Ce champ apparaît uniquement si un job a déjà été planifié pour cette tâche.

Nom du job

Spécifie le nom du job que vous souhaitez créer ou modifier.

Fuseau horaire

Spécifie le fuseau horaire du serveur.

Remarque : Si votre fuseau horaire est différent de celui du serveur, une liste déroulante permet de sélectionner votre fuseau horaire ou celui du serveur lorsque vous planifiez un nouveau job. Vous ne pouvez pas changer le fuseau horaire lorsque vous modifiez un job existant.

Planification quotidienne

Indique que le job se répète régulièrement après un certain nombre de jours.

Tous les (nombre) jours

Définit le nombre de jours s'écoulant entre deux exécutions du job.

Planification hebdomadaire

Spécifie que le job est exécuté un ou plusieurs jours spécifiques de la semaine, à une heure précise.

Jour de la semaine

Spécifie le ou les jours de la semaine où le job est exécuté.

Planification mensuelle

Spécifie un jour de la semaine ou du mois où le job s'exécute selon une base mensuelle.

Planification annuelle

Spécifie un jour de la semaine ou du mois où le job s'exécute selon une base annuelle.

Planification avancée

Spécifie les informations de planification supplémentaires.

Expression Cron

Pour obtenir des informations sur le remplissage de ce champ, reportez-vous à l'adresse suivante :

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

Heure d'exécution

Spécifie l'heure, au format 24 heures, à laquelle le job est exécuté. Par exemple, 14:15.

Exécution immédiate d'un job

Pour exécuter un job immédiatement, utilisez l'assistant Nettoyer les tâches soumises.

Dans l'onglet Système :

1. Sélectionnez Nettoyer les tâches soumises dans le volet gauche.

   La fenêtre Répétition de l'assistant s'ouvre.

2. Sélectionnez Exécuter, puis Suivant.

   La fenêtre Nettoyer les tâches soumises de l'assistant s'ouvre.

3. Entrez les informations relatives à l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de tâche, puis cliquez sur Terminer.

   Le job est soumis immédiatement.

Planification d'un nouveau job

Pour planifier un nouveau job, utilisez l'assistant Nettoyer les tâches soumises.

Dans l'onglet Système :

1. Sélectionnez Nettoyer les tâches soumises dans le volet gauche.

   La fenêtre Répétition s'ouvre.

2. Sélectionnez Planifier un nouveau job, entrez le nom et les informations de planification du job, puis cliquez sur Suivant.

   La fenêtre Nettoyer les tâches soumises s'ouvre.

3. Entrez les informations relatives à l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de tâche, puis cliquez sur Terminer.

   Le nouveau job est planifié.

Modification d'un job existant

Pour modifier un job existant, utilisez l'assistant Nettoyer les tâches soumises.

Dans l'onglet Système :

1. Sélectionnez Nettoyer les tâches soumises dans le volet gauche.

   La fenêtre Répétition s'ouvre.

2. Sélectionnez Modifier le job actuel et choisissez un job existant, modifiez les informations de planification, puis cliquez sur Suivant.

   La fenêtre Nettoyer les tâches soumises s'ouvre.

3. Modifiez les informations relatives à l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de tâche, puis cliquez sur Terminer.

   Le job existant est modifié.

Suppression d'une tâche récurrente

Pour supprimer une tâche récurrente, procédez comme suit :

Dans Afficher les tâches soumises

1. Sélectionnez Supprimer une tâche récurrente.
2. Sélectionnez la tâche que vous souhaitez supprimer.
3. Cliquez sur Soumettre.

Onglet Nettoyer les tâches soumises

Cet onglet permet de spécifier l'âge minimum, l'archivage, le délai d'expiration de l'audit, la limite de temps et la limite de la tâche. Lorsque tous les champs obligatoires sont remplis, cliquez sur Terminer. Cet onglet dispose des champs suivants.

Age minimal

Spécifie l'âge minimum des tâches dont l'état final (Terminé, Echec, Rejet, Annulation ou Abandon) doit être nettoyé. Par exemple, si 1 mois est spécifié, toutes les tâches ayant atteint un état final au cours du dernier mois sont conservées. Toutes les tâches ayant atteint un état final il y a plusieurs mois font l'objet d'un nettoyage et d'un archivage.

Ce champ est obligatoire.

Archiver

Sauvegarde les tâches dans l'archivage de la base de données avant suppression de la base de données d'exécution.

Une fois la tâche exécutée, si l'archive est sélectionnée, les données sont soumises à la base de données d'archivage et supprimées de la base de données de persistance des tâches d'exécution. Les données ne sont supprimées qu'une fois correctement soumises à la base de données d'archivage.

Délai d'expiration de l'audit

Spécifie le délai avant nettoyage des tâches présentant l'état Audit. Les tâches présentant l'état Audit n'atteignent pas l'état final tant que ce délai n'est pas écoulé. Les tâches présentant l'état Audit n'ont été soumises

Limite de temps

Limite le nettoyage à une durée spécifique.

Limite de la tâche

Limite le nettoyage à une nombre de tâches spécifique.

Suppression des tâches récurrentes

Lorsque l'exécution régulière d'une tâche n'est plus nécessaire, l'administrateur CA IdentityMinder peut la supprimer. Une fois cette opération effectuée, la collecte et l'archivage de déchets n'ont plus lieu pour cette tâche.

Toutes les tâches planifiées avec l'assistant Répétition dans Nettoyer les tâches soumises sont répertoriées sur cette page et l'administrateur CA IdentityMinder peut choisir la tâche à supprimer.

Remarque : Les tâches sont toujours présentes dans la base de données. Seule la récurrence de la planification est supprimée.

Configuration de la connexion CA Enterprise Log Manager

Utilisez cette fenêtre pour gérer les tâches de connexion de CA User Activity Reporting (UAR CA).

Remarque : CA Enterprise Log Manager a été renommé. Il est maintenant nommé CA UAR.

Les champs qu'elle contient sont répertoriés ci-dessous.

Nom de la connexion

Spécifie le nom unique utilisé pour l'objet géré de connexion CA UAR unique.

Il s'agit d'un champ en lecture seule.

Description

Décrit la connexion CA UAR.

Nom d'hôte

Spécifie le nom d'hôte ou l'adresse IP du serveur CA UAR.

Ce champ est obligatoire.

Nº de port

Spécifie le port de connexion du serveur CA UAR.

Valeur par défaut : 52 520

Ce champ est obligatoire.

Certificat SSL signé par une autorité de certification

Lorsque cette option est activée, elle spécifie une vérification de certificat SSL stricte lors de la connexion à un serveur CA UAR.

Si vous disposez d'un certificat SSL auto-signé, installé par exemple avec CA UAR par défaut, cette case à cocher ne doit pas être activée car le chemin approuvé vers l'autorité de certification racine n'existe pas.

Nom du certificat

Spécifie le nom du certificat CA UAR à utiliser pour l'authentification.

Ce champ est obligatoire.

Mot de passe du certificat

Spécifie le mot de passe CA UAR.

Ce champ est obligatoire.

Attribut

Non pris en charge. La version est récupérée lors d'une tentative d'enregistrement des informations de connexion comme test.

Suppression de la connexion Enterprise Log Manager

Sélectionnez une connexion dans la liste, puis cliquez sur Supprimer. La connexion à CA UAR est supprimée.

Gestion de clés secrètes

Utilisez des clés secrètes pour gérer les clés de chiffrement ou de déchiffrement des données. Si vous pensez qu'un utilisateur dispose d'un accès non autorisé à une clé, vous pouvez changer le mot de passe du magasin de clés. Le magasin de clés est la base de données de stockage des clés secrètes. Une fois que vous changez ce mot de passe, CA IdentityMinder chiffre de nouveau les valeurs des clés.

Procédez comme suit:

1. Entrez ou modifiez le mot de passe du magasin de clés.
2. Cliquez sur Ajouter une clé si vous avez besoin d'une autre clé.
3. Sélectionnez un algorithme.
4. Entrez un mot de passe pour la clé.

   Pour PBE et RC2, la longueur de clé maximum est de 128 octets.

   Pour AES, les tailles de clé valides sont 16, 24 et 32 octets.
5. Cliquez sur Soumettre.
6. Si vous avez modifié le mot de passe du magasin de clés, cliquez sur Soumettre.

   CA IdentityMinder chiffre de nouveau les valeurs des clés.

Index

G

I

J

M

V